2015

7th International Conference on Cyber Conflict:

Architectures in Cyberspace

M.Maybaum, A.-M.Osula, L.Lindström (Eds.)

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn Estonia

IEEE
*Advancing Technology
for Humanity*

26-29 MAY 2015, TALLINN, ESTONIA

2015 7TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE

IEEE Catalog Number:	CFP1526N-PRT
ISBN (print):	978-9949-9544-2-1
ISBN (pdf):	978-9949-9544-3-8

COPYRIGHT AND REPRINT PERMISSIONS

PRINTED COPIES OF THIS PUBLICATION ARE AVAILABLE FROM:

NATO CCD COE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Layout: Jaakko Matsalu

LEGAL NOTICE: This publication contains opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of NATO CCD COE, NATO, or any agency or any government. NATO CCD COE may not be held responsible for any loss or harm arising from the use of information contained in this book and is not responsible for the content of the external sources, including external websites referenced in this publication.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence is a NATO-accredited knowledge hub focused on interdisciplinary applied research and development as well as consultations, trainings and exercises in the field of cyber security. The Centre's mission is to enhance capability, cooperation and information-sharing between NATO, Allies and partners in cyber defence.

Membership of the Centre is open to all Allies. Currently, the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA have signed on as sponsoring nations. Greece and Turkey are working on finalising their accession process. Austria has become a contributing participant and Finland is well on its way to doing the same.

The Centre is staffed and financed by sponsoring nations and contributing participants. The Centre is not part of NATO command or force structure, nor is it funded from the NATO budget.

For more information, please visit the Centre's website at http://www.ccdcoe.org.

CYCON 2015 SPONSORS

TECHNICAL SPONSOR

IEEE

Advancing Technology for Humanity

DIAMOND SPONSOR

Microsoft

GOLD SPONSORS

CISCO™

SPONSORS

ixia

UK Trade & Investment

Raytheon

FOREWORD

This, the seventh annual International Conference on Cyber Conflict (CyCon 2015) organised by the NATO Cooperative Cyber Defence Centre of Excellence, has again been held in the historic city of Tallinn, the capital of Estonia. Over the years the CyCon conferences have proved to be world-recognised forums on advanced methods of modelling cyber conflicts and their strategic, legal and policy implications for society, business and world affairs. Every year, CyCon devotes its attention to a specific aspect of cyber conflict. In 2013, the conference discussed the roles and methods of automated cyber defence: it looked at automation, not only as an enabling technological field that allows for an increase in the effectiveness and sophistication of cyber defensive and offensive actions, but also as a social factor which touches on the political, legal, moral and ethical framework of modern society. In 2014, the conference concentrated on active cyber defence. The focus of CyCon 2015 is on the architectural aspects of cyberspace, from – as is true for all CyCon conferences – information technological, strategic, legal, and policy perspectives.

As cyber attacks and countermeasures are becoming more complex and sophisticated, it is time to take our understanding of the very nature of these attacks to the next level regarding how they impact the overall framework of personal, business, national, and international security and what are the best approaches to counter the threat. The mission of CyCon conferences is to look at the issues, models, and solutions for cyber conflict from a multi-disciplinary perspective.

We would like to thank both the members of the CyCon 2015 Programme Committee and the distinguished peer reviewers for their tireless work in identifying papers for presentation at the conference and for publication in this book. Last, but not least, we are delighted to congratulate the dedicated editors of this volume.

Programme Committee Co-Chairs

Dr Gabriel Jakobson
Chief Scientist, Altusys Corp

Dr Rain Ottis
Associate Professor
Tallinn University of Technology

Brookline, Tallinn, April 2015

TABLE OF CONTENTS

INTRODUCTION

For the seventh year in a row, the International Conference on Cyber Conflict (CyCon) has brought together national security thinkers, strategists, political scientists, policy-makers, lawyers, and technology experts interested in cyber defence, and has served as a hub for knowledge and networking on an international level.

CyCon 2015 – themed 'Architectures in Cyberspace' – focused on the construction of the internet and its potential future development. The main principles and foundations for the internet were laid four decades ago, and they have been used ever since. The 'net' has been a tremendous success story and today it is much more than just a commodity. However, can the structures that we rely on support the increasing demand and the different ways in which we want to use it, and what are the effects of this revolution on norms, international politics and security?

Building on these questions, this book contains selected articles that were presented during CyCon 2015.

The articles dedicated to the strategy and policy dimensions cover a wide array of topics. Deterrence in cyberspace has been one of the key issues at the strategic level for quite some time; **Jason Rivera** challenges the often-repeated claim that cyber deterrence is difficult or near impossible. His article aims to explain how even small and less powerful states can hold larger and more powerful states at risk in cyberspace. **Robert Brose** invites us to reflect on the concept of information warfare and its direct implications for cyber defence organisations today. Following up on the theoretical aspects of information warfare, **Margarita Jaitner** and **Peter A. Mattson** provide a case study of Russian information operations during the Ukraine crisis; they specifically explain the role of cyberspace in the broader Russian strategy for information warfare. **Tim Maurer et al**. take a closer look at the European proposals for technological sovereignty. Their article provides a comprehensive mapping and impact assessment of these proposals, covering both the technical and the non-technical, and evaluates how these proposals may protect against foreign surveillance. Finally, **Sergei Boeke et al**. take a look at how militaries in their own national contexts contribute to defensive cyber security across Asia and Europe. Common national challenges are identified, along with approaches to improve cyber security through better civil-military cooperation, specifically between Asia and Europe.

The articles that focus on the developments of international law offer insights into the possible interpretation of customary international law principles in the context of state behaviour in cyberspace. **Geoffrey DeWeese** offers a comprehensive definition of the notion of anticipatory self-defence under international law and discusses the challenges of its applicability in cyberspace. Similarly, **Paul Walker** advocates for an evolution of certain principles that govern the behaviour of states in cyberspace and focuses his article on state responsibility for an internationally wrongful act. He elaborates on the necessary changes to be applied to the concept of countermeasures as a way for states to deal with a majority of cyber attacks that do not reach the threshold of the use of force. Underlining the importance of international agreements and cooperation, **Uchenna Jerome Orji** follows with an analysis of the multilateral legal responses to cyber security threats in Africa. In particular, he looks at a range of regional instruments for cyber security and asks whether they are equipped to provide adequate frameworks for mutual assistance and international cooperation on cyber security and cybercrime control. Finally, **Richard Hill** explains his views on the future of the regulation of cyber security. His article advocates for the need for an international agreement on improving cyber security, and he discusses the role of the International Telecommunication Union in enhancing international cooperation in tackling cyber threats.

On the technical side, addressing the future challenges within the field of situational awareness, **Jennifer Stoll** and **Rainhard Bengez** lay out an implementation concept of visual structures for seeing cyber policy strategies: this aims to support information synthesis for policy actions by significantly reducing complexity and increasing information visibility. Their article examines publicly available analyses related to three types of security incidents: epidemics, cyber attacks on industrial networks and the threat of terrorist attacks. Continuing on how to address cyber incidents, **Alison Russell** takes a strategic perspective on the Anti-Access and Area-Denial (A2/AD) theatre in the physical layer of cyberspace and proposes means of deterrence, including the option to invest in resilience to counter a potential A2/AD strategy. Following up on this proposal, **Robert Koch** and **Mario Golling** identify the benefits of using Information and Communications Technologies in military operations and the importance of Network Centric Warfare (NCW) together with the danger of a potential failure resulting in an anti-access/area denial in cyberspace. The authors provide a synopsis of future technologies that might help mitigate the risk, along with recommendations on how to implement robust NCW improvements for its resilience.

Mirco Marchetti et al. focus on methods of supporting sense-making and decision-making through time evolution analysis of open sources. They propose a novel approach to managing, querying and visualising temporal knowledge extracted from unstructured documents. Based on a timed multigraph database, highlighting relationships between entities in different documents and in different time frames, they introduce a concept of temporal query that allows the analysis and visualisation of these relationships and their evolution over time.

Approaching the serious games topic, **Alexis Le Compte et al**. tackle the effectiveness of gamification for training and education purposes in cyber security. The authors argue that using serious games in formal and informal contexts would reach wider audiences while complying with national cyber strategies and achieving pedagogic results. A renewed framework is presented, based on existing practice and on methodologies for serious game design oriented towards those with a limited set of cyber security skills and knowledge. Serious games require serious adversaries possessing advanced techniques to execute cyber campaigns such as cyber espionage and information exfiltration. To explore this further, **Matteo Casenove** introduces in his paper a polymorphic blending exfiltration approach which in typical network conditions provides possibilities to evade signature and anomaly based detection. The paper shows how to blend data in the normal and legitimate traffic and how to detect such an exfiltration technique.

Lastly, **Christos Xenakis** and **Christoforos Ntantogian** describe the design and implementation of a new type of mobile malware attacking the baseband modem of smart phones by using described AT commands. This malware is capable of compromising the privacy of the user by stealing security credentials and sensitive information of the cellular technology, including permanent and temporary identifiers, encryption keys and the location of the smart phone, and using them for identification and tracking of the owner's movements and decrypting voice calls and data connections.

All of the articles in this book have gone through double-blind peer review by the Programme Committee. We would therefore like to thank the Co-Chairs as well as the distinguished members of the Programme Committee for their efforts in reviewing, discussing and selecting the submitted papers, guaranteeing their academic quality.

Programme Committee Co-Chairs:

- Prof Gabriel Jakobson, Altusys Corp
- Dr Rain Ottis, Tallinn University of Technology

Programme Committee Members:

- Dr Iosif Androulidakis, Ioannina University
- Bernhards Blumbergs, NATO CCD COE
- Cpt Pascal Brangetto, NATO CCD COE
- Dr Steve Chan, MIT/Harvard
- Prof Thomas Chen, Swansea University
- Dr Christian Czosseck, NATO CCD COE Ambassador
- Prof Dorothy E. Denning, Naval Postgraduate School
- Prof Gabi Dreo Rodosek, Bundeswehr University
- BGen Prof Paul Ducheine, Amsterdam University
- Dr Kenneth Geers, NATO CCD COE Ambassador
- Prof Michael Grimaila, AFIT
- Dr Jonas Hallberg, FOI
- Prof David Hutchison, Lancester University
- Maj Harry Kantola, NATO CCD COE
- Kadri Kaska, NATO CCD COE
- Prof Sokratis Katsikas, University of Piraeus
- Prof Jörg Keller, Hagen Open University
- Dr Marieke Klaver TNO
- Dr Scott Lathrop, USMA
- Dr Sean Lawson, University of Utah
- Corrado Leita, LASTLINE Inc
- Sam Liles, Purdue University
- Dr Lauri Lindström, NATO CCD COE
- Eric Luiijf, TNO
- Cpt Markus Maybaum, NATO CCD COE
- Prof Michael Meier, Bonn University
- Dr Jose Nazario, INVINCEA Inc
- Lars Nicander, Swedish National Defence College
- Anna-Maria Osula, NATO CCD COE

- Dr Patryk Pawlak, EU Institute for Security Studies
- Raimo Peterson, NATO CCD COE
- Maj Nikolaos Pissanidis, NATO CCD COE
- Henry Rõigas, NATO CCD COE
- Prof Juha Röning, Oulu University
- Julie J.C.H. Ryan, Georege Washington University
- Lt-Col Jan Stinissen, NATO CCD COE
- Dr Jens Tölle, Fraunhofer FKIE
- Dr Enn Tõugu, Tallinn University of Technology
- Lorena Trinberg, NATO CCD COE
- Dr Risto Vaarandi, NATO CCD COE
- Teemu Uolevi Väisänen, NATO CCD COE
- Lt-Col Jens van Laak, NATO CCD COE
- Matthijs Veenendaal, NATO CCD COE
- Dr Jozef Vyskoc, VAF
- Prof Bruce Watson, Stellenbosch University
- Dr Sean Watts, Creighton University
- Prof Stefano Zanero, Milan University

Special thanks are due to the Institute of Electrical and Electronic Engineers (IEEE): the IEEE Estonia Section served as a technical co-sponsor for CyCon 2015 and this publication. Numerous IEEE members have supported the Programme Committee, ensuring the academic quality of the papers and supporting their electronic publication and distribution.

A big thank you also goes to Jaanika Rannu from NATO CCD COE, without whose organising skills and skilful eye this publication would probably not have made it to print.

Last but not least, we would like to thank the authors of the papers published here and presented during CyCon 2015 for their excellent submissions and friendly cooperation during the course of the publication process.

The CyCon 2015 Agenda Management Board

Bernhards Blumbergs
Cpt Pascal Brangetto
Lauri Lindström
Cpt Markus Maybaum
Anna-Maria Osula
Maj Nikolaos Pissanidis
Henry Rõigas
Matthijs Veenendaal
Teemu Uolevi Väisänen

NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia, April 2015

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk*

Jason Rivera
Deloitte & Touche LLP
Threat Intelligence & Analytics
Captain, United States Army National Guard
Georgetown School of Foreign Service
Washington, D.C., United States
jhr47@georgetown.edu

Abstract: Achieving cyberdeterrence is a seemingly elusive goal in the international cyberdefense community. The consensus among experts is that cyberdeterrence is difficult at best and perhaps impossible, due to difficulties in holding aggressors at risk, the technical challenges of attribution, and legal restrictions such as the UN Charter's prohibition against the use of force. Consequently, cyberspace defenders have prioritized increasing the size and strength of the metaphorical "walls" in cyberspace over facilitating deterrent measures.

The notion of cyberdeterrence is especially daunting when considering how small states can deter larger, militarily more powerful states. For example, how would Estonia or Japan conduct deterrence through cyberspace against larger regional adversaries with more robust military capabilities? The power disparities between nations of such different military stature are seemingly overwhelming and insurmountable. It is these disparities in cyber power that present conceptual challenges, especially when measuring power in terms of military size, budget, strength, and technological capabilities.

"Power," however, is a broad term that should be considered beyond the military context. This is especially true in cyberspace, where a nation without a strong military can hold a militarily powerful nation at risk, so long as the former is aware of their strategic advantages as well as the critical vulnerabilities of the latter.

Given this reality, this paper shall suspend, or at least cast reasonable doubt on, the notion that cyberdeterrence is either difficult or impossible. Using a deductive method to analyze the components of cyberdeterrence strategy and examine the various challenges involved, this

* All views and concepts expressed in this paper originate solely with the author and do not represent the official positions or opinions of the U.S. Army National Guard, the U.S. Department of Defense, or Deloitte & Touche LLP.

paper introduces a hypothesis on how small, less powerful states can hold large powerful states at risk through cyberspace.

Keywords: *attribution, cyberdeterrence, deterrence, use of force*

1. INTRODUCTION

Cyberdeterrence strategy remains largely unexplored and underdeveloped, due to a limited understanding of how the principles of deterrence can be applied to the cyber domain. Because cyberspace has only recently become an object of national security focus, the development of cyber theory relative to the other domains of warfare is relatively immature. In a broad sense, cyberspace warfighting strategy today is analogous to the growth of air power strategy during the interwar period between World Wars I and II. While the U.S. is actively developing doctrine, mobilizing forces, and allocating resources, there is still much to be done in developing comprehensive cyberspace warfighting strategies.

This paper defines cyberdeterrence as the mechanism through which nation-states can communicate proportionate, reciprocal, and credible military power effects through cyberspace that strategically affect their adversary's decision making calculus. The specific aim of cyberdeterrence is to deter an adversary from conducting hostile actions through cyberspace, although its application could be much broader. For example, a cyberdeterrent could be used to dissuade an adversary from conducting hostile conventional military actions, or even to gain diplomatic leverage.

Four prevailing viewpoints have arisen in the body of work on cyberdeterrence:

1. Cyberdeterrence is difficult but potentially achievable, through the ability to hold the adversary's critical cyberspace security objectives at risk.[1]
2. Cyberdeterrence is difficult and potentially unachievable, due to technical restraints pertaining to attribution.[2]
3. Cyberdeterrence is legally unattainable, due to the UN Charter's prohibition on the use of force and domestic laws that forbid response actions at the substate echelon.[3]
4. Cyberdeterrence is difficult if not impossible to achieve, as any measures taken are unlikely to deter potential adversaries; resources would be better spent pursuing other defensive means.[4]

Acknowledging that these viewpoints outline the challenges of cyberdeterrence, this paper offers the following hypothesis:

A nation-state, regardless of its size or military strength, can achieve cyberdeterrence if it can hold an adversary's critical cyberspace security objectives (CSOs) at risk[a] by communicating its own retaliatory or autonomous cyberspace capability.

[a] The term "hold at risk" should be understood as the means through which nations leverage military capabilities in order to threaten critical national security objectives of other nation-states.

1. If the deterrence capability is retaliatory,
    a. the deterring nation-state need only attribute nefarious actions to the IP space of the adversarial state;
    b. the capability likely would not violate the UN Charter's prohibition against the use of force if it does not violate national sovereignty, does not damage/destroy people or objects, and does not provide weaponry or training to organized actors.

2. If the deterrence capability is autonomous,
    a. the deterring nation-state need not conduct attribution;
    b. the capability may be acceptable if it does not violate the UN Charter's prohibition against the use of force or domestic law forbidding unauthorized network access.

2. HOLDING A LARGE STATE'S CRITICAL CYBERSPACE SECURITY OBJECTIVES AT RISK

A. National Cyberspace Security Objectives

According to realist theory, anarchy forces states to compete for power because that is the best way to achieve security, and achieving security is the only way to ensure survival. This concept is no different in cyberspace, and it applies to the security objectives of nation-states within the cyber domain. In *People, States*, and *Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Barry Buzan cites two principle lenses through which states view their security interests: their ability to leverage military power and their internal socio-political cohesion.[6] In his article 'The Cyber Threat to National Security: Why Can't We Agree?' military strategist and author Forrest Hare argues that these two lenses also heavily affect a nation-state's security objectives in cyberspace.[7] These two lenses divide states into four broad categories:

1. Powerful states with more socio-political cohesion
2. Powerful states with less socio-political cohesion
3. Less powerful states with more socio-political cohesion
4. Less powerful states with less socio-political cohesion

In table 1, Hare sums up states' cyberspace vulnerabilities based on their socio-political cohesion and military strength.

TABLE 1[8]

		Socio-political Cohesion	
		Less Socio-Political Cohesion	More Socio-Political Cohesion
Power	Less Powerful	Destabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDoS and major attacks on critical infrastructure
	More Powerful	Destabilizing political actions in cyberspace	Criminal activities in cyberspace

Hare's table can be used to categorize states according to their greatest perceived threats in the cyber domain, which in turn can be leveraged to hold an adversarial state at risk. Subsequently, these perceived threats indicate a state's most valuable Cyberspace Security Objectives (CSOs). Expanding on this concept, this paper assumes that humanity inherently aspires to be safe, free, generally private, and unoppressed by their governments. CSOs that promote these aspirations are inherently positive, whereas those that detract from these aspirations are inherently negative. States that pursue only positive CSOs do not fear internal insurrection and likely have strong socio-political cohesion. States that pursue negative CSOs likely fear internal insurrection, which indicates a lower degree socio-political cohesion. To classify these objectives further (see table 2), this paper draws from statements by Melissa Hathaway, former director for cyberspace at the U.S. National Security Council, that pertain to security-related aims in cyberspace:

TABLE 2[9]

Positive CSOs	Negative CSOs
1. The promotion of Internet freedom: freedom of speech, content hosting, and browsing	**1. The restriction of Internet freedom:** censorship, controlling content, shaping opinions, forbidding opposition ideas
2. Promoting the availability of services: preventing denial of service, combating malware, etc.	**2. Controlling popular unrest:** restrictions on social media coordination, web-forum gatherings, etc.
3. Combating cybercriminals: identity theft, data breach, hacking, Internet predators	**3. Promoting lawlessness in cyberspace:** crime facilitation, corruption, lack of accountability for actions in cyberspace
4. Combating industrial espionage: copyright adherence, defense of intellectual property	**4. State-sponsored industrial espionage:** copyright violations, intellectual property theft

By understanding these CSOs, one can categorize nation-states and enumerate which equities can be held at risk through cyberdeterrence. This categorization is fundamental to a small state's ability to hold a large state at risk: *understanding the adversary's critical cyberspace security objectives is the most important aspect of leveraging a viable cyberdeterrence strategy*. Consider, for example, the series of cyberattacks in November-December 2014, allegedly conducted by North Korea against the United States' entertainment industry. By conducting devastating attacks against a company's network, invoking memories of 9/11, and indirectly threatening moviegoers, North Korea, which is militarily less powerful than the U.S., directly deterred the U.S. commercial sector's capacity to exercise freedom of speech.[10] The effect of this cyberspace deterrent was the direct denial of positive CSO one: the promotion of Internet freedom. This paper will continue to expand on this core concept as the various aspects of cyberdeterrence are analyzed.

B. State Categorization

Using the Buzan/Hare model, nation-states can be categorized in terms of socio-political cohesion and cyber power. This paper proposes four such categories:[b]

1. *States with more socio-political cohesion and more powerful cyberwarfare programs:* These states support all positive CSOs, do not support negative CSOs, and can be held at risk if their positive CSOs are threatened.

2. *States with more socio-political cohesion and less powerful cyberwarfare programs:* These states support all positive CSOs, do not support negative CSOs, and can be held at risk if their positive CSOs are threatened.

3. *States with less socio-political cohesion and more powerful cyberwarfare programs:* These states support one or more negative CSOs and can be held at risk if their negative CSOs are threatened.

4. *States with less socio-political cohesion and less powerful cyberwarfare programs:* These states support one or more negative CSOs and can be held at risk if their negative CSOs are threatened.

Drawing on these four categories, table 3 presents a sample of nation-states categorized by cyber power and socio-political cohesion:

TABLE 3

		Socio-political Cohesion[c]	
		Less Socio-Political Cohesion	More Socio-Political Cohesion
Cyber Power[d]	Less Powerful	Bahrain, Belarus, Malaysia, Morocco, Venezuela	Belgium, Denmark, Estonia, Japan, New Zealand, Panama
	More Powerful	China, Egypt, Iran, North Korea, Pakistan, Russia	Australia, Brazil, Germany, India, Israel, U.K., U.S.

[b] A listing of 77 categorized nations can be found in the appendix of this paper.

[c] The author defines the term "socio-political cohesion" as a function of civil liberties and political rights, as measured by Freedom House's yearly publication, *Freedom in the World*.

[d] Cyber power measured as a function of military power, status of cyber warfare capabilities, and relative strength compared to regional competitors.

Table 3 provides a tool for determining an effective way to hold a nation's critical CSOs at risk. Estonia and Japan, for example, both support the positive CSOs and are not known to support any negative ones. Both countries are in the less powerful cyber power category, due to having cyberwarfare programs that fall short of those of their primary regional rivals. History demonstrates that Estonia, for example, can be held at risk by an ability to deny positive CSO number two: promoting the availability of services. This disparity was made evident in 2007 when patriotic Russian hackers allegedly conducted distributed denial of service (DDoS) attacks against Estonian websites, causing a major disruption in Estonian governance. Japan is also vulnerable to large and militarily more powerful actors and, as a result, continually experiences cyberattacks from more powerful entities. In 2014, approximately 25 billion cyberattacks were reported to have taken place against the Japanese government, with approximately 40 percent of them traced to regional rivals.[11] This is an exponential increase from the 2005 total of 310 million, when the first Japanese national cyberattack survey took place.[12]

Those nations in the lower left quadrant of table 3, in contrast, are categorized as strong cyber powers due to their heavy investment in military, intelligence, and law enforcement cyber equities. These nations are unlikely to be held at risk in the same manner as Estonia or Japan, due to their robust capabilities. However, to combat internal socio-political shortcomings, these nations subsequently support negative CSOs. For example the Russian Business Network (RBN) actively supports negative CSO three: the promotion of lawlessness in cyberspace. The RBN is a well-known and relatively blatant supporter of cybercrime that is alleged to have ties to Russian politics; its known nefarious activities include the creation of malware, spam centers, illegal pornographic content, botnets, and monopolization of the market for stolen identities.[13] Two recent and potentially significant examples of such cybercrimes are the point-of-sale identity theft attacks that have been plaguing the retail sector, which were confirmed to have contained the BlackPOS malware with embedded materials that suggest links to a cybercriminal network.[14] These activities and their possible links to politics imply that a deterring entity could hold an aggressor at risk if it could expose the links between criminal and political actors.

Other countries, in contrast, have strict Internet laws and practices designed to control content. For example, according to Section Five of China's Computer Information Network and Internet Security, Protection and Management Regulations, no unit or individual may use the Internet to engage in "making falsehoods or distorting the truth, spreading rumors, destroying the order of society [or] injuring the reputation of state organs."[15] This has led to the widespread filtering of web servers or domain name IP addresses, Domain Name Server redirection, and keyword filtering.[16] These sorts of measures imply that a government that supports negative CSO number one, the restriction of Internet freedom, could be held at risk if a deterring entity were capable of "enabling" unrestricted Internet freedom to the restrictive government's population.

C. Retaliatory and Autonomous Capabilities

The capacity to hold an adversary's critical CSOs at risk is paramount to this paper's hypothesis. Once these security objectives are identified, the deterrer must then develop, communicate, and, if necessary, deploy a capability that can fulfill its cyberdeterrence objective. In terms of deterrent actions, a nation-state is generally capable of levying either retaliatory or autonomous capabilities.

A *retaliatory deterrence capability* is one that falls in line with Martin Libicki's notion of "the need to develop a capability in cyberspace to do unto others what others may want to do unto us."[17] Employing this capability insinuates a response-focused cyberdeterrence mechanism that threatens the adversary with use of force if it continues to conduct nefarious actions. Retaliatory responses, in general, are problematic on two fronts. First, they require a certain extent of attribution. Precise attribution is problematic with currently available technology and will likely be so in the immediate future. Second, a retaliatory response may require the threat of use of force, which violates article 2(4) of the UN Charter's prohibition against the use of force. These problems will be discussed later in this paper, but it should be made clear that levying a retaliatory capability requires the deterrer to address attribution and legal concerns.

A deterrer also can leverage *autonomous deterrence capabilities*, which are mechanisms that do not require active response or counteroffensive actions to be effective, such as a firewall or a honeynet. At a minimum, a firewall or honeynet will force a nefarious actor to expend valuable time. It is even better if the firewall reports the IP address of those attempting an intrusion, or if the honeynet reveals the attacker's methodologies and tools. Autonomous capabilities, while potentially less effective than retaliatory capabilities, have a lower threshold in terms of attribution requirements and conform more with international legal norms.

Both retaliatory and autonomous capabilities must be communicated to an adversary in a way that effectively demonstrates that the deterrer can harm their CSOs. However, the deterrer must not communicate its capability in a way that allows the adversary to render it useless. An adversary who censors the Internet, for example, must be made to believe, via deterrence communication channels, that the deterrer is able to restrict or eliminate the adversary's capacity to censor the web. Similarly, an adversary state that sponsors industrial espionage must believe that the deterrer has the cyber capability to harm it if it continues to support espionage activities.

3. ATTRIBUTION AND CYBERDETERRENCE

One key challenge in achieving cyberdeterrence is the notion of attribution. The attribution problem has technical and human components, and both can be challenging. Technical attribution includes analyzing malicious code, functions, and packets and then leveraging this analysis to locate the networked node where the nefarious activity originated.[18] Human attribution involves leveraging the results of technical attribution to identify an organization or person responsible for the nefarious activity.[19] In both cases, attribution is not an end in itself but a means for holding the adversary's critical cyber equities and objectives at risk. Because attribution is a means, not an end, this paper disputes the notion that one must unequivocally identify the adversary's location and networks to achieve deterrence. To levy a retaliatory capability, one need only conduct attribution back to the IP space of the offending nation-state, which is achievable with currently available technology. If using an autonomous capability, the deterring state need not confirm attribution, since the capability will autonomously levy adverse effects against intruding adversaries.

A. Retaliatory Capabilities and Attribution

The nature of state-sponsored cyber activity suggests that attribution can be achieved in tiers. U.S. Senator Sheldon Whitehouse suggests that tiered attribution can be achieved as follows: nation → region → city → group → individual.[20] Cybersecurity firm Mandiant's exposure of Advanced Persistent Threat 1 illustrates this concept. Starting with suspected Chinese state-sponsored industrial espionage activities, Mandiant managed to narrow down the aggressors to → large-scale infrastructure in Shanghai → specific fiber optic infrastructure provided by state-owned enterprise China Telecom → PLA Unit 61398 → specific individuals.[21] This demonstrates attribution for nefarious activities from the nation-state echelon down to the individual. However, to achieve cyberdeterrence a nation-state need not attribute blame to the individual but to the responsible state, thus it would have been sufficient to attribute the nefarious actions back to the country in which the Internet service provider was hosted.

The capacity for a small state to achieve attribution against a large state is especially relevant in the discussion of retaliatory capabilities. Far too often, small states see the inability to gain precise attribution as a non-starter for employing retaliatory capabilities, but this simply need not be the case. In the article 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks,' Jason Healey notes that "analysts often fall into the trap of 'attribution fixation,' the belief that they cannot assess which organization or nation was behind an attack until technical forensics discovers the identity of the attacking machines."[22] Healey adds that "knowing 'who is to blame?' can be more important than 'who did it?' Moreover, attribution becomes far more tractable when approached as a top-down policy issue with nations held responsible for major attacks originating from their territory or conducted by their citizens."[23] It logically follows that nation-states are almost always (wittingly or unwittingly) responsible for cyber aggression ranging from the IP space of their geographic borders. Table 4 juxtaposes a spectrum of state responsibility with historical incidents of cyber aggression.

TABLE 4

Spectrum of State Responsibility[24]	Historical Example
1. State-prohibited: National government will help stop third-party attacks.	In 2002, the U.S. Federal Bureau of Investigation creates a Cyber Division to combat cyber-based terrorism, foreign intelligence operations, and cybercrime.[25]
2. State-prohibited-but-inadequate: National government is cooperative but unable to stop the third-party attacks.	In 2014, a report indicate that the United States, despite having stringent Internet law enforcement measures, is host to approximately 40% of malware serving botnets, more than any other country in the world.[26]
3. State-ignored: National government knows about the third-party attacks but is unwilling to take any official action.	In 2007, "patriotic hackers" conduct DDoS attacks against Estonian state websites.
4. State-encouraged: Third parties control and conduct the attack, but the national government encourages them as a matter of policy.	Around 2007, Iran creates the Basij Cyber Council to organize Iranian civilian hackers under the supervision of the Iranian Revolutionary Guard Corps.[27]
5. State-shaped: Third parties control and conduct the attack, but the state provides some support.	The Syrian Electronic Army, a group that supports the Syrian regime and likely receives some state support, hacks into several news producing entity.[28]
6. State-coordinated: National government coordinates third-party attacks, such as by "suggesting" operational details.	In 2008, Russia sponsors website "StopGeorgia.ru," which encourages the hacker population to engage targets within Georgian web space.[29]
7. State-ordered: National government directs third-party proxies to conduct attacks on its behalf.	In 2005-2007, in an effort to delay the Iranian nuclear program, the United States, under the George W. Bush administration, allegedly initiates an effort code-named Olympic Games,[30] and coordinates with third-party Israeli proxies to plant USB devices in key Iranian nuclear facilities.[31]
8. State-rogue-conducted: Out-of-control elements of government cyber forces conduct the attack.	In 1999, after the accidental bombing of the Chinese embassy in Belgrade, rogue hacker elements from Russia, Latvia, Lithuania, and Serbia conduct anti-NATO cyberattacks.[32]
9. State-executed: National government conducts attack using cyber forces under their direct control.	In 2007, Israeli forces infiltrate Syrian air space and destroy the al-Kibar nuclear reactor by triggering a kill-switch installed in Syrian air defense radar systems.[33]
10. State-integrated: National government attacks using integrated third-party proxies and government cyber forces.	For the last decade, several government entities have used third parties to conduct targeted exfiltration attacks against firms and major industries to enhance their economy and defense industry.[34]

This section demonstrates that the attribution threshold for deploying retaliatory capabilities only requires a nation-state to attribute nefarious actions back to the IP space of the offending state. Even if malicious actors employ proxies in third-party countries to conduct cyberattacks, the third-party nation still has the responsibility to act. Healey once coined the term "Cyber Somalia," which refers to a tendency in the international community to treat cyberattacks "as if every country were Somalia: helpless to restrain attacks from its territory or mitigate their downstream impacts."[35] This is simply not the case. States, especially highly capable and technologically developed states, typically have the law enforcement means to assume responsibility for actions within their borders.

B. Autonomous Capabilities and Attribution

Whereas the physical domain is characterized by variations in the terrain, cyberspace is characterized by environmental variables, including the emplacement of and interaction between routers, switches, servers, firewalls, and transmission mediums. One central difference from the physical domain is that cyberspace is manmade and therefore can be altered, which is the premise on which autonomous capabilities not focused on attribution can be leveraged.

Autonomous capabilities can support a small nation-state's pursuit of cyberdeterrence if the deterrer correctly conducts organizational characterization and predictive cyberthreat analysis. Organizational characterization will help the deterrer understand the equities that a nefarious adversary may threaten; predictive cyberthreat analysis will help the deterrer understand the tactics, methods, and means the adversary will most likely use. Once a deterrer achieves organizational understanding and can reasonably predict the nature of a cyberthreat, attribution is no longer required, as the deterrer will have the knowledge needed to levy an autonomous capability. Table 5 presents examples of autonomous cyberdeterrent capabilities that do not require attribution.

TABLE 5

Organization	Cyberthreat	Autonomous Cyberdeterrent Capability
Intelligence Agency	Hacktivist conducting website defacement	Firewall with attached intrusion prevention system that conducts reverse IP address look up of nefarious actor; broadcasts location of all proxy IP addresses and actors to law enforcement forces, thereby degrading anonymity.
Host-Nation Military	Adversarial military force conducting offensive operations	Intentionally seed deterrer's network with malware so that when data is exfiltrated back through the ISP of the aggressor country, the ISP's ability to censor the Internet or social media is degraded, thereby hampering the strategic objectives of autocratic states.

4. LEGAL CONSIDERATIONS AND CYBERDETERRENCE

A. Legal Considerations of Retaliatory Capabilities

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the most comprehensive work outlining the international laws and norms of cyberspace in accordance with the UN Charter. This section of the paper focuses in particular on *Tallinn Manual* Rule 10: Prohibition of Threat or Use of Force: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[36]

Taking into account the *Tallinn Manual*, a deterrer considering using a retaliatory capability will need to comply with two things: the UN Charter's prohibition on the use of force and the non-intervention principle. Compliance is critical, as deterrence actions occur before hostilities begin, and thus, are generally recognized as not covered under the right to self-defense and must not be characterized by the use of force. As for the non-intervention principle, article 2(7) of the UN Charter states that "the United Nations has no authority to intervene in matters which are within domestic jurisdiction of any State."[37] The *Tallinn Manual* states that "the fact that a cyber operation does not rise to the level of a use of force does not necessarily render it lawful under international law."[38] A good example of crossing the non-intervention threshold is when the U.S. provided training and weapons to the Contras in Nicaragua. Although the U.S. was not directly involved in kinetic operations, in 1986 the International Court of Justice ruled that U.S. actions constituted a use of force.[39]

Table 6 gives examples of what the *Tallinn Manual* would and would not consider state-sponsored use of force.

TABLE 6[40]

Use of Force	Below Use-of-Force Threshold
Cyber actions that kill people or damage/destroy objects	Conducting psychological operations designed to undermine confidence in government or economy
Providing an organized group with malware and the requisite training to conduct a cyberattack	Funding a hacktivist group conducting cyber operations as part of an insurgency
Training an organized group to conduct a cyberattack	Granting sanctuary to non-state actors to conduct cyber operations
Providing sanctuary in addition to cyber defenses for a non-state group	Failing to police territory and prevent launch of cyber operation by non-state actors

In addressing the four retaliatory capabilities listed above in the "below use-of-force" column, a full-fledged cyber power will be unable to levy the "Cyber Somalia" excuse within the international community. This means that granting sanctuary or failing to police a state's territory are not viable options. Moreover, funding a "hacktivist" organization will require leasing control of national-level CSOs to unpredictable and unquantifiable entities, which would defeat the purpose of conducting proportional, reciprocal, and credible deterrence operations. Therefore, to achieve cyberdeterrence using a retaliatory capability while adhering to the *Tallinn Manual*'s guidance on the use of force, deterrers should levy psychological operations within the cyber domain. Psychological cyber operations should be designed to have a widespread effect on the targeted nation's populace while remaining below the threshold of force.

The notion of CSOs was referenced above as the key cyber aim point needed to hold an adversary at risk. Therefore, an examination of the suitability of retaliatory capabilities should be premised on how these objectives are held at risk and whether the retaliatory capability in question crosses the use-of-force threshold. Table 7 presents some retaliatory psychological operations capabilities that could be deployed against adversaries with negative CSOs that would not cross the use-of-force threshold.

TABLE 7

Potential Adversary & Activity in Support of a Negative CSO	Retaliatory Deterrence Capability That Is below Use-of-Force Threshold
A government entity that monitors online content and communications through a centralized location in the regime's telecommunications monopoly.[41]	Enable externally hosted search engines outside of the jurisdiction of a nations ISPs, thereby negating the government's ability to censor web searches.[42]
In response to ongoing protest activity, a government that blocks and degrades content on popular social media websites.	Provide proxy access to unrestricted social media websites, thereby enabling the population's ability to coordinate ideas and protest against the government.
Large government entities known for their heavy concentration of corrupt bureaucrats that are responsible for the facilitation of cybercrime syndicates.	Expose intelligence-related information that provides proof of corrupt relations between government officials and cybercriminals.

Note that a retaliatory capability that does not violate the UN prohibition on the use of force may not necessarily imply that the capability is in compliance with article 2(4) of the UN Charter. Any action that violates nation-state sovereignty or intervenes in domestic affairs may still be prohibited, even if such actions are akin to the national intelligence collection process levied by nations throughout the world. Therefore, levying a retaliatory cyberdeterrence capability requires decision makers to make a conscious decision on their usage and therefore accept the potential of a negative outcome.

B. Legal Considerations of Autonomous Capabilities

If a deterrer is operating at the substate echelon, it is critical that it stays within both international law and the boundaries of domestic law—especially when leveraging autonomous capabilities. There is a strong inclination, particularly in Western law, to outlaw unauthorized access to computer networks, known as hacking. This includes "hack-backs," private companies that attempt to retaliate against cybercriminals in order to deter crime, steal back information, shut down the assailant's network, or seek revenge. For example, 18 U.S. Code § 1030 states that "knowingly access[ing] a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information," is illegal.[43] Given this restriction, it is critical that autonomous cyberdeterrent capabilities not be dependent on gaining unauthorized access.

To abide by domestic law, the deterrer must execute cyberdeterrence functions from within its own network. Thus when the deterrer's network has been compromised, it should implement internally based cyberthreat countermeasures (IBCC), which are designed to autonomously levy a negative response against an adversary.[44] The organization levying an IBCC would be required to act within legal constraints. In the U.S., for example, title 10 (military) and title 50 (intelligence) organizations have the legal authority to employ malware in the execution of their roles.[45] Examples of autonomous capabilities that could be used by those with the legal authority to employ malware appear in table 8.

TABLE 8

Deterring Organization	Adversary	Threatening Action through Cyberspace	Autonomous Deterrence Capability
Intelligence Agency	Rival Intelligence Agency	A foreign intelligence agency conducts operations to exfiltrate valuable national security data.	Intentionally host malware within the deterrer's intelligence agency network; when that malware is exfiltrated to the rival intelligence agency's network, the malware opens up a back door, allowing the deterrer's organization to conduct Computer Network Exploitation (CNE).
Law Enforcement Agency	Organized Criminals	Groups of organized criminals conduct financial crimes against a deterring nation's citizens and corporations.	Flood the Internet with intentionally hosted proxy networks, applications, and web forums that attract users within the organized crime echelons. An example of such a service is the Silk Road, a Tor hidden service designed to allow users to anonymously conduct illicit trade activities online. When those proxy networks, applications, and web forums have gained sufficient bona fides, push Trojan updates to those hosted entities that compromise the computers of the organized criminals and subsequently reveal their location and activities.

Other entities may not have the legal authority to host malware but nonetheless be critical to a nation-state's cyberspace security posture. These include the defense industrial base, information technology, telecommunications, energy sectors, etc. These sectors may be required to levy autonomous deterrents that affect the risk calculus and operational strategy of the adversary, as opposed to infecting the adversary's networks with malware. Examples of such capabilities are presented in table 9.

TABLE 9

Deterring Organization	Cyberthreat	Threatening Action through Cyberspace	Autonomous Deterrence Capability
Defense Industrial Base (DIB)	Intellectual Property Thief	In order to gain a competitive advantage, a foreign military conducts industrial espionage through cyberspace.	Develop a honeynet that includes intentionally seeded and flawed information designed to sow confusion, misdirection, false intent, and deception. For the DIB, honeynets should contain technology/personnel counter-data that is relevant, yet disadvantageous to an adversary.[46]
The Energy Sector	Terrorists	Terrorists seeking to cause chaos attempt to gain access to the electrical power grid by using a sniffer on a network in order to compromise electrical power company usernames and passwords.	Develop and deploy software that would make it so, that for every legitimate login attempt that took place, the software would simultaneously fabricate additional username and password attempts across the network. The aim would be that the employee endpoint terminal itself would be unable to differentiate between the legitimate login attempt and the fabricated login attempt. Login attempts would be transmitted via encrypted channels to a highly secure central processing location, and fabricated login attempts would be sent to another centralized database. If a criminal/terrorist entity were to use fabricated login data to log in to the close network, it would be flagged and thus cue law enforcement authorities.[47]

5. CONCLUSION

This paper has discussed the plausibility of cyberdeterrence and the challenges in achieving it. By breaking down the various challenges, which include the ability to hold the adversary at risk, the notion of attribution, and the need to operate within legal norms, the paper gives credence to its hypothesis that cyberdeterrence can be achieved, and that even small nation-states can achieve it using retaliatory and autonomous capabilities. Small states can levy retaliatory capabilities to achieve deterrence so long as they can attribute nefarious actions to the IP space of the adversarial state and the retaliatory capability does not violate the UN prohibition on the use of force. Alternatively, small nation-states can achieve cyberdeterrence using autonomous capabilities, which do not require attribution and can be leveraged in conformity with article 2(4) of the UN Charter as long as they violate neither the UN prohibition on the use of force nor domestic law forbidding unauthorized network access.

Cyberdeterrence, like conventional deterrence, centers on understanding the adversary's center of gravity, having a threatening capability, and communicating to the adversary the willingness to unleash the capability if a red line is crossed. To position the cyberspace environment to their advantage, cybersecurity practitioners at both the interstate and substate echelons should integrate cyberdeterrence into their defensive plans.

6. APPENDIX

Nation-State[e]	**Military Power Index**[f] [48]	**Presence of Government Sponsored Cyberwarfare Programs**[49]	**Political Rights**[50]	**Civil Liberties**[51]
Argentina*	2		High	High
Australia+*	4	Yes	High	High
Austria*	3		High	High
Azerbaijan	2		Low	Low
Bahrain	1		Low	Low
Bangladesh	2		Medium	Medium
Belarus	2		Low	Low
Belgium*	3		High	High
Bolivia	1		Medium	Medium
Brazil+*	4	Yes	High	High
Bulgaria*	1		High	High
Canada+*	4	Yes	High	High
Chile*	2		High	High
China+	5	Yes	Low	Low
Colombia	2		Medium	Medium
Croatia*	2		High	High

[e] The + symbol = strong cyber power relative to adversaries; the * symbol = relatively strong socio-political cohesion.

[f] 5 = most powerful; 4 = highly powerful; 3 = powerful; 2 = less powerful; 1 = minimally powerful

Czech Republic*	3	Yes	High	High
Denmark*	3		High	High
Ecuador	1		Medium	Medium
Egypt	4		Low	Medium
Estonia*	1	Yes	High	High
Finland*	2		High	High
France+*	5	Yes	High	High
Georgia	2		Medium	Medium
Germany+*	5	Yes	High	High
Greece*	2		High	High
Hungary*	2		High	High
India+*	5	Yes	High	Medium
Indonesia*	4		High	Medium
Iran+	4	Yes	Low	Low
Israel+*	4	Yes	High	High
Italy+*	4	Yes	High	High
Japan*	4	Yes	High	High
Jordan	2		Low	Medium
Kazakhstan	1		Low	Medium
Kenya	2	Yes	Medium	Medium
Kuwait	1		Medium	Medium
Lebanon	1		Low	Low
Lithuania*	1		High	High
Malaysia	3		Medium	Medium
Mexico	3		Medium	Medium
Morocco	2		Medium	Medium
Netherlands*	3	Yes	High	High
New Zealand*	1	Yes	High	High
Nigeria+	3	Yes	Medium	Medium
Norway*	3		High	High
Oman	1		Low	Medium
Pakistan	4	Yes	Medium	Medium
Panama*	1		High	High
Peru*	2		High	Medium
Philippines	3		Medium	Medium
Poland*	4	Yes	High	High
Portugal*	2		High	High
Qatar	1		High	High

Romania*	2		High	High
Russia+	5	Yes	Low	Medium
Saudi Arabia+	3	Yes	Low	Low
Serbia*	2		High	High
Singapore	3	Yes	Medium	Medium
Slovenia*	1		High	High
South Africa+*	3	Yes	High	High
South Korea*	4	Yes	High	High
Spain*	3		High	High
Sweden*	3	Yes	High	High
Switzerland*	3		High	High
Syria+	3	Yes	Low	Low
Thailand	3		Medium	Medium
Tunisia	2		Medium	Medium
Turkey+	4	Yes	Medium	Medium
Ukraine	3		Medium	Medium
United Arab Emirates	3		Low	Low
United Kingdom+*	5	Yes	High	High
United States+*	5	Yes	High	High
Uruguay*	3		High	High
Uzbekistan	2		Low	Low
Venezuela	2		Medium	Medium
Vietnam	3		Low	Medium

REFERENCES

[1] Forrest Hare, ‘The Significance of Attribution to Cyberspace Coercion: A Political Perspective’ 4th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2012), 131.

[2] Dmitri Alperovitch, ‘Towards Establishment of Cyberspace Deterrence Strategy’ 3rd International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2011), 91.

[3] Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Colorado Springs, CO: U.S. Air Force Academy, 1999), 17.

[4] Gregory Rattray and Jason Healey, ‘Categorizing and Understanding Offensive Cyber Capabilities and Their Use’ Proceedings of a Workshop on Deterring Cyberattacks (Washington, DC: National Academies Press, 2010), 88.

[5] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton & Company, 2011), 50.

[6] Barry Buzan, *People, States, & Fear: An Agenda for International Security Studies in the Post-Cold War Era* (London, UK: ECPR Press, 1991), 134.

[7] Forrest Hare, ‘The Cyber Threat to National Security: Why Can’t We Agree?’ 2nd International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2010), 218.

[8] Ibid.

[9] Melissa Hathaway, ‘Developing International Norms for a Safe, Stable, and Predictable Cyber Environment’ Georgetown University Conference on International Engagement on Cyber, March 4, 2014.

[10] Jason Rivera, ‘North Korea Has Crossed the Cyber Red Line by Combining Cyberattacks with the Threat of Terrorism—and the United States Must Respond’ (2014) *Georgetown Security Studies Review* http://georgetownsecuritystudiesreview.org/2014/12/18/north-korea-has-crossed-the-cyber-red-line-by-combining-cyberattacks-with-the-threat-of-terrorism-and-the-united-states-must-respond/ (accessed 19 Dec. 2014).

[11] British Columbia, ‘Security News Digest’ http://www.cio.gov.bc.ca/local/cio/informationsecurity/pdf_securitynewsdigest/02_24_2015.pdf (accessed 16 Mar. 2015).

[12] Ibid.

[13] RBN Exploit ‘Russian Business Network (RBN)’ HostExploit, 2014. http://rbnexploit.blogspot.com/ (accessed 4 Nov. 2014).

[14] Brian Krebs, ‘Home Depot Hit by Same Malware as Target’ krebsonsecurity.com, 2014. http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ (accessed 4 Nov. 2014).

[15] U.S. Embassy Beijing, ‘New PRC Internet Regulations’ Federation of American Scientists, 1998. https://www.fas.org/irp/world/china/netreg.htm (accessed 6 Apr. 2014).

[16] Jonathan Zittrain and Benjamin Edelman, ‘Empirical Analysis of Internet Filtering in China’ Harvard Law School, Berkman Center for Internet and Society, 2003. http://cyber.law.harvard.edu/filtering/china/ (accessed 6 Apr. 2014).

[17] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 27.

[18] W. Earl Boebert, *A Survey of Challenges in Attribution* (National Academies Press Online 2010), 44.

[19] Ibid.

[20] U.S. Senator Sheldon Whitehouse (Rhode Island), Comments made at Georgetown University Conference—International Engagement on Cyber: Developing International Norms for a Safe, Stable, and Predictable Cyber Environment, March 4, 2014.

[21] Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units* (Mandiant 2013), 19.

[22] Jason Healey, ‘Beyond Attribution: Seeking National Responsibility for Cyber Attacks’ Atlantic Council, Cyber Statecraft Initiative (Washington, DC: Atlantic Council, 2012), 1.

[23] Ibid.

[24] Ibid., 2.

[25] ‘Ten Years After: The FBI Since 9/11,’ FBI website, 2014. http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber (accessed 19 Apr. 2014).

[26] Jaikumar Vijayan, ‘US Tops List of Countries Hosting Malware and Botnets’ securityintelligence.com, 2014. http://securityintelligence.com/news/us-tops-list-of-countries-hosting-malware-and-botnets/#.VQa82PnF-So (accessed 16 Mar. 2015).

[27] U.S. House Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, ‘Iranian Cyber Threat to the U.S. Homeland’ April 26, 2012. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm (accessed 19 Apr. 2014).

[28] DHS Office of Cybersecurity & Communications, ‘Cyber News Spotlight: Insight on Cybersecurity News & Trends for Critical Infrastructure’ http://www.htcia.org/wp-content/uploads/Cyber-News-Spotlight-February-2014.pdf (accessed 16 Mar. 2015).

[29] Andreas Hagen, ‘The Russo-Georgian War 2008’ in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 197.

[30] Dorothy Denning, ‘Stuxnet: What Has Changed?’ (2012) 4 *Future Internet*, 673.

[31] Joshua Kopstein, ‘Stuxnet Virus Was Planted by Israeli Agents Using USB Sticks, According to New Report’ *The Verge*, 2012. http://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran (accessed 19 Apr. 2014).

[32] Jonathan Diamond, ‘Early Patriotic Hacking,’ in Jason Healey (ed.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 138-139.

[33] ‘Significant Cyberattack Incidents: Operation Orchard, 2007’ Real Clear Politics, 2013. http://www.realclearpolitics.com/lists/cyber_attacks/op_orchard.html (accessed 16 Apr. 2014).

[34] Ibid., 21.

[35] Healey, ‘Beyond Attribution: Seeking National Responsibility for Cyber Attacks’, 4.

[36] Michael Schmitt et al., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press 2013), 45.

[37] UN Charter, art. 2, para. 7.

[38] Ibid., 46.

[39] International Court of Justice, ‘Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*, 1986)’ www.icj-cij.org. http://www.icj-cij.org/docket/index.php?sum=367&p1=3&p2=3&case=70&p3=5 (accessed 22 Apr. 2014).

[40] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 48-49.

[41] Patricia Figliola et al., ‘U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology’ Congressional Research Service (Washington, DC: GPO 2011), 10.

[42] Jason Rivera, ‘Understanding and Countering Nation-State Use of Protracted Unconventional Warfare’ (2014) *Small Wars Journal* http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare (accessed 24 Dec. 2014).

[43] 18 U.S.C. § 1030: US Code—Section 1030: Fraud and related activity in connection with computers.

[44] Jason Rivera and Forrest Hare ‘The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures’ 6th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications 2014), 109-110.

[45] Andru Wall, ‘Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action’ *Harvard National Security Journal* 3 (2012), 118.

[46] Rivera & Hare, ‘The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures’, 112.

[47] Ibid., 113.

[48] Global Fire Power, ‘Countries Ranked by Military Strength,’ www.globalfirepower.com, 2014. http://www.globalfirepower.com/countries-listing.asp (accessed 9 May 2014).

[49] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O’Reilly Media, Inc., 2011), 243-261.

[50] Arch Puddington, *Freedom in the World 2014* (Washington, DC: Freedom House 2014), 18-22.

[51] Ibid.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Cyberwar, Netwar, and the Future of Cyberdefense

Robert Brose
Office of the Director of National Intelligence[1]
Washington D.C., United States of America

Abstract: Over twenty years ago, Arquilla and Ronfeldt warned that both "Netwar" and "Cyberwar" were coming, and could impact the 21st Century security landscape as significantly as combined arms maneuver warfare had impacted the security landscape of the 20th. Since that time, the concept of "Cyberwar" has received great attention, while the parallel concept of "Netwar" has languished, even as its salience to global security has continued to grow. This paper suggests that just as Cyberdefense organizations have been required to confront Cyberwar, Netwar organizations, or Netwar-savvy Cyberdefense organizations, are increasingly needed to counter Netwar. Revisiting the Netwar concepts of the 1990s, it offers a 21st century Netwar definition; examines Netwar from a non-western perspective, exploring intersections between Netwar and Russian concepts of 'Information-Psychological,' Chinese United Front Theory, and Chinese Legal Warfare, and concludes with thoughts on unique roles that today's Cyberdefence organizations may play in future Netwar conflict.

Keywords: *cyberwar, netwar, information-psychological, united front theory*

1. INTRODUCTION

In the summer of 1993, a twenty-page article titled "Cyberwar is coming!" anticipated many of the challenges that western national security practitioners would encounter in years to follow. The paper featured an inspired emphasis on the socially-transforming effects of information technology suggesting "…the information revolution is strengthening the importance of all forms of networks, such as social networks…"[2]; anticipated that cyber-concepts could transform the role of militaries, imagining a day when militaries would conduct "hitting without holding"[3]; and included an eerie forecast of future crises' in which the U.S. might face "large, well-armed irregular forces, taking maximum advantage of familiar terrain, motivated by religious, ethnic, or tribal zeal… [and able to] move easily within and between the "membranes" of fractionated

[1] The author of this paper is the Lead for Futures and Capability Development at the U.S. Office of the Director of National Intelligence (ODNI). The author prepared this work as a conceptual thought piece as part of his official U.S. Government duties. However, this paper should not be interpreted as an official policy, policy statement, or endorsement, either expressed or implied, of ODNI or the U.S. Government. This paper is a U.S. Government work. The U.S. Government hereby claims all applicable copyright protection under the laws of any country in which this paper is reproduced, published, or distributed.

[2] John Arquilla and David Ronfeldt, *Cyberwar is Coming!* in COMPARATIVE STRATEGY, Vol. 12, No. 2, Spring 1993, pp. 141–165, 144.

[3] *Id*. at 157.

states."[4] As the centerpiece of this article, authors John Arquilla and David Ronfeldt, then of the RAND Corporation but speaking on their own behalf, defined Cyberwar and Netwar as two emergent forms of warfare meriting greater study.[5]

Since that time, Cyberwar – the act of "disrupting, if not destroying, information and communication systems…on which an adversary relies in order to know itself…"[6] – has received substantial attention, from practitioners, policymakers, industry, and security theorists. However, if Cyberwar served as the bright 'Yang' of the paper, its' shadowy 'Yin' counterpart was Netwar, in which actors overtly and covertly sought to "…disrupt, damage, or modify what a target population knows or thinks it knows about the world around it."[7] It is this darker, less clearly bounded and potentially more profound challenge to the security of open and democratic nations that this paper focuses on in detail, first offering an updated definition of Netwar, then highlighting Russian and Chinese doctrinal concepts that may be applied in Netwar, and finally concluding with thoughts on how western actors may re-purpose or adapt traditional cyber organizations for Netwar defence.

2. NETWAR, THEN AND NOW

"Whereas Cyberwar refers to knowledge-related conflict at the military level, Netwar applies to societal struggles most often associated with low-intensity conflict…"[8]

The early concepts put forward by Arquilla and Ronfeldt focused for the most part on what they termed Cyberwar – impacts of emerging *network technologies* on conventional warfare, and the implications of attacks on the interdependence and transformative connectivity that would result. Of the twenty pages in the article, only a few address Netwar, and the thinking is less developed, but enough emerges from the document to make the following distinctions:[9]

1. Although it may be conducted in *concert with* Cyberwar, Netwar is qualitatively different from Cyberwar; while Cyberwar targets information systems, Netwar targets societal self- and world-perceptions;
2. Netwar may be pursued through any combination of diplomacy, propaganda, psychological campaigns, political and cultural subversion, deception or interference with local media, and efforts to promote dissident or opposition movements via computer networks;
3. Netwar may also involve infiltration of computer networks and databases, but if "this leads to targeting an enemy's military C3I capabilities" the action has crossed from Netwar to Cyberwar.

This thinking has since evolved and been refined by the global cyber security community (Arquilla and Ronfeldt included,) but the prevailing focus has remained Cyberwar. Martin Libicki, writing in *Strategic Studies Quarterly*, provides a refresh of the Cyberwar concept, but seems to view Cyberwar as an activity predominantly undertaken to support "combat in the physical domain,"[10] and the Tallinn Manual on the International Law Applicable to Cyber

[4] *Id*. at 160.
[5] *Id*. at 141.
[6] *Id*. at 146.
[7] *Id*. at 144.
[8] *Id*. at 141.
[9] *Id*. at 144-145.
[10] Martin C. Libicki, *Why Cyber War Will Not and Should Not Have Its Grand Strategist*, STRATEGIC STUDIES QUARTERLY, Volume 8, No 1 (2014).

Warfare[11] defines 'Cyber' as the "networked technology" itself, 'warfare' as the "use of force," and acknowledges that it does not address cyber activities "below the level of 'use of force'."[12] Yet, would any national security scholar or practitioner dispute that at least some components of Netwar – for example, deliberate combinations of diplomacy, propaganda, and manipulation of media – seem to be growing in the modern geopolitical space? And do we not recognize an increasing potential for delivery of psychological campaigns to our doorstep, and the mobilization of 'dissident or opposition movements,' whether at the behest of state or non-state actors, via the Internet? If so, then we must also acknowledge that Netwar has in fact emerged alongside Cyberwar, and offer a definition of it that can enable a more effective and insightful analysis of current events than is possible without it.

3. A WORKING DEFINITION OF MODERN NETWAR

I offer the following as a working definition of Netwar in the 21st Century:

1. *Netwar consists of intentional activities to influence the domain of human perception via either overt or hidden channels, in which one or more actors seeks to impose a desired change upon the perception of another actor, in order that this change facilitate second-and third order effects of benefit to them;*
2. *Netwar does not imply a resort to physical force, non-cooperative modification of digital data, or even, necessarily, an act that violates any written laws of the targeted actor or the present-day international system;*[13]
3. *Discrete actions within a Netwar may include collective, personal, or machine-generated speech or action, economic choices, or other legally protected activities, in addition to acts of information conveyance, distortion, or denial that may or may not violate laws or sovereignty.*

This is a broad definition, not entirely discontinuous from US doctrinal descriptions of "Diplomatic, Informational, Military, and Economic" (DIME) power, and NATO descriptions of "Cyber operations" conducted as a component of "state power."[14] However, while Netwar may entail the use of cyber systems and tools as conduits, it is not "employment of cyber capabilities with the primary purpose of achieving [military] objectives,"[15] but instead the utilization of cyber (or social) systems as infrastructure supporting perceptual manipulation aimed at "achieving strategic goals."[16]

This broad definition also highlights the challenge of Netwar: employment of the 'M' in DIME may violate the UN Charter, intersect NATO article 5, or justify a range of 'out of band' responses, but a Netwar "attack" on target perceptions, conducted without attributable use of military force, presents the target with fewer internationally acceptable responses – particularly if they are unprepared, or unable, to respond via a Netwar of their own. It is this very asymmetry

[11] Michael N. Schmitt (ed.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, United Kingdom, Cambridge University Press, 2013, 3.

[12] *Id*, at 4.

[13] Cyberwar activities of the 'Cyber-on-Cyber' variety – when they do occur – may facilitate Netwar, or be conducted in parallel to Netwar, as may be kinetic forms of warfare, but these are not acts of Netwar in and of themselves.

[14] "Fighting Power, Targeting and Cyber Operations" in THE 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS, NATO CCDCOE Publications, Tallinn, Estonia, 2014, 307.

[15] Michael N. Schmitt, *supra* note 11 at 258, and in Paul Ducheine and Jelle van Haaster, *Id*. at 304.

[16] Paul Ducheine and Jelle van Haaster, *Id*. at 305.

of means-legitimacy which a shrewd Netwar practitioner may exploit, and which the following sections explore.

4. NETWAR IN EASTERN PERSPECTIVE

While western national security practitioners may lack a "Grand Strategist" of Netwar, to paraphrase Martin Libicki,[17] their eastern counterparts have several to choose from. Qiao Liang and Wang Xiangsui's relatively recent treatise, *Unrestricted Warfare*[18], provides some hints at the deeper theoretical reservoir an eastern strategist might draw upon, but was perhaps better understood as a critique of U.S. – or extant Chinese – methods through an orientalist lens. As some western reviewers have noted, *Unrestricted Warfare* represented "neither a revolution in military thought nor an executable doctrine for future warfare but a collection of tactics, techniques, and procedures that have been used throughout history."[19]

For deeper insight, a modern day Netwar practitioner must look farther into the past. From the 64 discrete socio-political conditions described - albeit in semi-mystical terms - within the I-Ching, to the more widely read *Art of War* by Sun-Tzu, Oriental classics offer a wealth of anecdotally expressed thinking on how disparate influences may be brought to bear on an opponent, deflecting, co-opting, or "defeating" them without resort to physical violence. It has become cliché for western authors to cite Sun-Tzu's aphorism that "to defeat an enemy without fighting is the acme of skill,"[20] [21] and then treat the concept superficially, but the very words an English speaker employs in translation may distort the understanding of the concepts; in English defeat implies overthrow, downfall, conquest, and rout.[22] In contrast, study of Chinese history suggests Sun-Tzu would have likely included *any outcome that allowed the protagonist to significantly advance their interests* as a 'defeat' for the opponent, and recognized the possibility of 'opponent' to become ally or neutral party in an instant[23] (in other words, *it is the state of effective opposition*, not the entity themselves, that must necessarily be defeated.)

In the traditional eastern perspective every entity is perpetually vying for advantage within a sea of competitive forces, and competition with others is not a discrete (or moral) act to be initiated against a select set of 'bad guys' or 'evil-doers', but an eternally present and universal fact, which any rational actor denies at their peril. As George Kennan wrote, in describing the Soviet Union of 1947, *"...its political action is a fluid stream which moves constantly, wherever it is permitted to move, toward a given goal. Its main concern is to make sure that it has filled every nook and cranny available to it in the basin of world power. But if it finds unassailable barriers in its path, it accepts these philosophically and accommodates itself to*

[17] Libicki, *supra* note 10.

[18] Qiao Liang and Wang Xiangsui, UNRESTRICTED WARFARE, PLA Literature and Arts Publishing House, China, 1999.

[19] Major John A. Van Messel, USMC, *Unrestricted Warfare: A Chinese doctrine for future warfare?* (Submitted in partial fulfillment of the requirements for the degree of Master of Operational Studies, United States Marine Corps School of Advanced Warfighting, 2005).

[20] Dean Cheng, "Winning a War Without Fighting," THE WASHINGTON TIMES, July 19, 2013, accessed at http://www.heritage.org/research/commentary/2013/7/winning-a-war-without-fighting.

[21] Arquilla and Ronfeldt themselves likely alluded to Sun-Tzu when they described Cyberwar as an act in which one disrupts means "an adversary relies in order to know itself…"

[22] MICROSOFT Word Thesaurus (search for "defeat").

[23] See various stories recounted in the Chinese classic ROMANCE OF THE THREE KINGDOMS, or 'San-Guo'

them."[24] From this perspective, "defeats" are seldom absolute, nor is a "victory" – or alliance - decisive. Thus, Sun-Tzu's aphorism might be alternately translated as 'the accomplishment of objectives through persistent persuasion, dissuasion, and manipulation is preferable to a resort to conflict in the physical domain' – a mission statement that seems well-aligned with the proposed definition of Netwar.

Strategists like Sun-Tzu are creatures of an ancient past, and at first glance, may seem several orders-removed from today, but if one looks at the 20th Century writings and actions of eastern powers, one can find concepts bridging the gap between these primeval concepts and the present. These include Russia's "Information Psychological," and the Chinese concepts of United Front Theory and Legal Warfare. Although each is different, they hold in common the basic premise that something resembling Netwar can and should be conducted in service of state objectives, and their study can serve as both tools to understand foreign perspective, and as concepts to inform modern Netwar.

5. INFORMATION-PSYCHOLOGICAL

"Excessive data do not enlighten the reader or the listener; they drown him. He cannot remember them all, or coordinate them, or understand them; if he does not want to risk losing his mind, he will merely draw a general picture from them. And the more facts supplied, the more simplistic the image…"[25]

Just as *Unrestricted Warfare* serves as a landmark for westerners seeking an entrée into the world of Chinese strategic thought, a recent article by Russian General Valery Gerasimov has of-late served to crystallize western awareness of asymmetric – or 'hybrid' - warfare as an emerging Russian forte. Writing in a 2013 issue of Voenno-promyshlennyi kur'er, or the *Military-Industrial Courier*, then Chief of the General Staff Gerasimov suggested that the "nonmilitary means of achieving political and strategic goals," which he characterized as "political, economic, informational, humanitarian, and other nonmilitary measures — applied in coordination with the protest potential of the population," were beginning to exceed traditional "kinetic" means in their net effectiveness.[26] Often referred to as the "Gerasimov Doctrine," this article has sometimes been described in the west as "prophetic"[27] in nature, but in reality merely summarizes and reframes the last fifteen years of evolution in Russian Military thinking. In his 2005 overview of global Information Operations concepts *Cyber Silhouettes*, Timothy Thomas noted that circa 2000, Russian military doctrine had already begun to differentiate between two forms of information conflict, acts of "Information Technical" and acts of "Information Psychological." *Information Technical* was associated with concepts that approximate today's western concepts of Cyberwar - "…technical intelligence devices, means and measures for protecting information, super-high-frequency weapons …radio-electronic

[24] George F. Kennan, The Sources of Soviet Conduct quoted in Alexander J. Motyl *The Sources of Russian Conduct: the New Case for Containment*, FOREIGN AFFAIRS 16 November, 2014, accessed at http://www.foreignaffairs.com/articles/142366/alexander-j-motyl/the-sources-of-russian-conduct.

[25] Jacques Ellul, Propaganda: The Formation of Men's Attitudes, New York: Knopf, 1965 on WIKIPEDIA accessed at http://en.wikipedia.org/wiki/Jacques_Ellul.

[26] Valery Gerasimov, *The Value of Science in Prediction* in The 'Gerasimov Doctrine' and Russian Non-Linear War, by Mark Galeotti's blog "In Moscow's Shadows," accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[27] Sam Jones, Ukraine: *Russia's new art of war*, FINANCIAL TIMES, 28August 2014, accessed at http://www.ft.com/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html#axzz3TdT0UrNC.

countermeasures, electromagnetic impulse weapons, and special software and hardware."[28] In contrast, *Information Psychological* was associated with use of the mass-media, and with the employment of "nonlethal weapons, psychotronic tools, and special pharmaceuticals." While these latter exotica fall outside the scope of this paper, study suggests Russia is using the mass-media, per *Information Psychological*, in its historic and present-day conduct of Netwar.

Whatever capabilities of propaganda the Soviet Union may have built up in the years preceding, a robust *Information Psychological* capability was lacking during the early years of post-Soviet Russian state. During the 1994-1996 period of the Chechen conflict, the Russian military failed to take an active part in generating content to fill the global media space, and when it did communicate to the media, did so haphazardly.[29] Russian journalists – at the time still relatively free from state control[30] - received both preferential access, and even funding for minor expenses, from a Chechen community spanning national borders as they reported on the conflict. Meanwhile, Russia's Chechen adversaries deployed mobile television production teams to support a dedicated Ministry of Information. In the words of Russian Major General Zolotarev, "the Chechen campaign of 1994-1996 by military definition was three-quarters won by the Russian Army by August 1996, but by that time it had lost 100% in infospace."[31] It was this era of Netwar *failure* that drove the next stage in Russian thinking.

By 1999 – just before the emergence of *Information Psychological* in the open literature – Russia demonstrated an ability to execute at least components of a Netwar in Chechnya. The Russian military supplied videos and briefing material through centers established in areas that were serving as staging areas for Russian journalists in the neighboring republics of Dagestan and North Ossetia.[32] Russian authorities also censored any content deemed adversary propaganda, initially shutting off independent reporting, and then maintaining bans of certain types of content throughout the conflict.[33] By the end of 1999, a new centralized Russian Information Center (RIC) was filtering content from the theatre of operations, and information from any foreign publications to be disseminated inside Russia,[34] with relatively crude censorship approaches complemented by shaping of themes and the tone of coverage associated with the Russian military itself, at least when directed at the domestic population. Emil Pain, a Russian trained ethno-sociologist and an "advisor to the Russian Federation President since

[28] Timothy Thomas, CYBER SILHOUETTES, Fort Leavenworth KS, Foreign Military Studies Office, 2005, 79.

[29] *Id*. at 183.

[30] *Id*. at 82.

[31] *Id*. at 183.

[32] *Id*. at 82.

[33] *Id*. at 184.

[34] The timing of RIC establishment *generally* coincides with both Vladimir Putin's assumption of the Presidency, and with a formal "Resolution 1538" (R-1538) of the Russian President. However, there is divergence in western accounts regarding the timing of both R-1538 and the stand-up of the RIC, raising the possibility that the "resolution" may have actually served to retroactively legitimize an *Information Psychological* fait-accompli. Thomas cites December of 1999 as the date for R-1538, and implies the RIC soon followed, while Paul Rich, writing in Crises in the Caucasus: Russia, Georgia, and the West (Routledge, 2013) claims the RIC was established by a "Governmental decree of 7 October." Suggesting even greater lag between RIC establishment and R-1538, French IO expert Daniel Ventre (who highlights the resolutions' parallel role in strengthening the powers of Russia's Federal Security Bureau) gives 7 February 2000 as the date of R-1538 [see Daniel Ventre, INFORMATION WARFARE, (United Kingdom, ISTE Ltd, and United States of America, John Wiley and Sons, 2009),] while Google's cache holds a 13 January 2000 *Voice of Russia* interview with *then RIC-head* Mikhail Margelov, stating that the RIC had been "opened on October 1st by the government."

1996,"[35] noted that by 2000, the very terminology used to describe the conflict had shifted. The Army was described as simply "working" in Chechnya, with the assaults it conducted termed "special operation[s]." Addressing the strategic approach that was being undertaken, Pain suggested Russia had initiated a deliberate strategy to "reprogram the mass consciousness" by promulgating new psycho-perceptual models of the world, to include a "new [type of] war" model, and a "Free Chechen" model, in which the Chechen people eagerly sought Russian liberation.[36]

By 2003, Russian military theorist S. P. Rastorguyev offered a description of information-centric conflict in which the final objective was to effect the knowledge of a specific information system (in context, clearly meant to include both machines and persons,) and the purposeful use of that knowledge to *"distort the model of the victim's world."* Clarifying that both target and means could be other-than-digital, Rastorguyev defined an information weapon as *"…any technical, biological, or social means or system that is used for the purposeful production, processing, transmitting, presenting, or blocking of data and or processes that work with the data."*[37] The same year, writing in Russia's Military Thought, S.A. Bogdanov suggested the goals of contemporary armed struggle were obtainable by a combination of "military, economic, and 'information-technical' and 'information-psychological' means,[38] suggesting the potential for Russian integration of Netwar with Cyberwar and traditional conflict. Thus, in Netwar per Bogdanov, one would expect to see the use of military power as a means to shape perceptions of a target audience (either in concert with, or absent traditional acts of violence); use of economic levers; and use of mass-media a-la *Information Psychologica*l, all integrated under a coherent strategy. A lesser, mere execution of *Information Psychological* alone, would at a minimum seek to engage mass media in the struggle, and seek to use it to distort target perceptions to Russian advantage.

However, Moscow faced difficulty in transforming these concepts into tools that worked reliably outside Russia. Writing in *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money*, authors Pomerantsev and Weiss suggest that when Russian authorities attempted to ensure victory for Viktor Yanukovych, a pro-Russian candidate in the 2004 Ukrainian elections, they found themselves unable to dominate the perceptual environment. As a result, at least one Russian media operative was forced to flee Ukraine in disguise as the Orange Revolution brought Victor Yuschenko to power. And four years later, during Russia's conflict with Georgia, despite securing services of external public relations firms and establishing the Russia Today (RT) television channel, Russian elites still perceived a failure to achieve victory in the external information domain.[39]

Perhaps in response to this weakness, structures Russia used to manage Netwar were once again revised. A position for a Presidential Special Advisor for Information and Propaganda Activities was established, and conduits under state control were expanded to include international "Non"-Governmental Organizations working alongside the Russian information

[35] "Biography of Emil Pain" (Stanford University) accessed 5 December 2014 at http://web.stanford.edu/group/Russia20/pain_bio.htm..

[36] Timothy Thomas, *supra* note 28 at 185.

[37] S. P. Rastorguyev in *Id*. at 78.

[38] S. A. Bogdanov, "The Probable Appearance of Future Warfare," (Voyennaya Mysl [Military Thought], 15 December 2003) as translated and downloaded from the FBIS website in May 2005, in *Id*. at 79.

[39] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York, Institute of Modern Russia, 2014, 12.

agencies and "information troops made up of state and military news media"[40] By 2010, Rear Admiral Pirumov was already anticipating Gerasimov's more recent assertion that "wars are no longer declared and, having begun, proceed according to an unfamiliar template,"[41] describing information 'warfare' as an activity that would be conducted in *both wartime and peacetime*, with a goal of securing "national policy objectives" through exerting influence on an opponent's information systems and "psychic conditions"; via promulgation of disinformation; societal and situational manipulation; "crises control"; propaganda efforts directed at effecting "conversion, separation, demoralization, desertion, [and] captivity"; lobbying; and blackmail.[42] President Putin himself reinforced this conceptualization of an eternal battle of influence when he described "soft power" as consisting of a "matrix of tools and methods to reach foreign policy goals … by exerting information and other levers of influence."[43] [44]

At present, many believe this type of *Information Psychological* is being actively practiced by Russia. Michael John Williams, an Associate Scholar at the Center for European Policy Analysis, citing Gerasimov, Bogdanov, and Russian strategist Sergey Chekinov, describes something much like *Information Psychological* as the first of two phases in modern Russian conflict, suggesting that in phase one "…unconventional operations are undertaken to manipulate public opinion at home, in the target country and foreign press. Eventually Russian forces, under the guise of domestic militants, will be deployed. This marks the end of the unconventional operations. If successful, the Kremlin then uses legal language to legitimate the intervention as one protecting "human rights" in the target country. The second phase is thus a much more conventional operation. In the case of Crimea, the operation was so successful that the conventional deployment barely required a shot to be fired."[45] Canada's Foreign Minister Baird summarized the situation more succinctly, and with a focus on aspects of *Information Psychological* directed farther abroad, suggesting Russia was "…polluting the opinion-making process in the west…[via]…the active manipulation of information."[46]

Russia's Netwar tools are diverse: RT has expanded to include multilingual news, a wire service, radio channels, and enjoys a budget measured in the hundreds of millions of dollars.[47] "Voice of Russia" has re-branded itself as "Sputnik," and is establishing a network of media hubs in 30 cities abroad,[48] echoing the establishment of the media centers during the Chechen conflict. Some researchers suggest Moscow also employs armies of online "trolls" to supplement these overt channels, using multiple social media accounts to participate in online discussions, and recruiting thousands of Twitter followers under multiple online identities.[49] The existence

[40] *Id*. at 12 and citing Igor Panarin in Timothy Thomas, RECASTING THE RED STAR, Foreign Military Studies Office, 2011.

[41] Valery Gerasimov, *supra* note 26.

[42] V.S. Pirumov, Informatsionne Protivoborstvo. Moscow, 2010, 3 quoted in Timothy Thomas *supra* note 39 and Peter Pomerantsev and Michael Weiss, *supra* note 39 at 12.

[43] Putin's concept of "soft power," which closely approximates Netwar, stands in contrast to western views of "soft power" as a normative attraction derived from actions making one desirable as a model or ally.

[44] Peter Pomerantsev and Michael Weiss, *supra* note 39, at 12.

[45] Michael John Williams, *Russia's New Doctrine: How the Kremlin Has Learned to Fight Tomorrow's War Today*, Center for European Policy Analysis, 09 May 2014, accessed at http://cepa.org/content/russia%E2%80%99s-new-doctrine-how-kremlin-has-learned-fight-tomorrow%E2%80%99s-war-today.

[46] John Baird, *Address by Minister Baird to the NATO Council of Canada Conference - Ukraine: The Future of International Norms*; 18 November 2014 - Ottawa, Ontario" accessed at http://www.international.gc.ca/media/aff/speeches-discours/2014/11/18b.aspx?lang=eng.

[47] Peter Pomerantsev and Michael Weiss, *supra* note 39 at 12.

[48] Stephen Ennis, *Russia's global media operation under the spotlight*, BBC NEWS ONLINE EUROPE, 16 November 2014, accessed at http://www.bbc.com/news/world-europe-30040363.

[49] Peter Pomerantsev and Michael Weiss, *supra* note 39 at 17.

of such obscured meme amplification architectures may explain propagation of supposedly "leaked" satellite images purporting to show that Flight MH17 was downed by a Ukrainian aircraft, even as other online communities noted inconsistencies and brand the images fake.[50] However, arguments of "real" or "fake" may miss the underlying intent of *Information Psychological*. Pomerantsev and Weiss suggest Moscow *"...exploits the idea of freedom of information to inject disinformation into society ... not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods [and] ... exacerbate divides."*[51] Fiona Hill, of the Brookings Institution is more direct, suggesting that *"Putin is aiming for that large swathe of the population, especially in the United States, that is non-conformist and deeply suspicious of their own government. Then in Europe there are those who follow populists on the far right and far left who are very prone to seeing their own governments as traitors to the national cause, or inept or overbearing."*[52] If these hypotheses are correct, the west should expect coordinated targeting of issues and communities pre-disposed to question domestic authority, and to accept – or at least entertain – alternate narratives that serve Moscow's interest. Information Psychological is thus not a logical contest, but an emotional contest for the hearts and minds of the swing votes and interests in targeted systems. And it is here that United Front Theory most clearly comes into play.

6. UNITED FRONT THEORY

"Cooperate with anybody who is not opposing us today, even though he did so only yesterday."[53] United Front Theory is, in simplest form, a strategy of a deliberately (and dynamically) shifting the boundary between ideological friend and foe in order to maximize the community aligned with a protagonist while isolating an opponent. Lyman Van Slyke, who chronicled the evolution of this approach within the Chinese Communist Party (CCP), suggests it emerged as a CCP tactic during the early 1920s,[54] [55] when CCP members (then a tiny minority) sought dual membership in the more powerful Nationalist Kuomintang (KMT) party as a means to initially reach, and ultimately co-opt, a greater number of followers.[56]

United Front Theory served as a useful tool to both guide and rationalize CCP policy regarding relations with, and accommodation to, the KMT. Toward the end of World War Two, Mao Tse-Tung suggested that in areas controlled by the KMT, Chinese communists should engage an extant social movement "…embracing various social strata…" and "…cooperate with anybody who is not opposing us today."[57] Here we see a willingness to put aside past conflict to realize a shared aim, but we should not read into this any intent of Mao to reach lasting accommodation

[50] Will Stewart and Amy Ziniak, *Were MH17 'satellite images' photoshopped? Report slams new surveillance pictures released by Russian state broadcaster as a 'shoddy fake'* MAIL ONLINE AND DAILY MAIL AUSTRALIA, 16 November 2014, accessed at http://www.dailymail.co.uk/news/article-2836245/Report-slams-new-surveillance-photos-released-Russian-state-broadcaster-MH17-shot-shoddy-fake.html.

[51] Peter Pomerantsev and Michael Weiss, *supra* note 39.

[52] Mark Franchetti, Toby Harnden and Michael Sheridan, *Kremlin Calling*, THE SUNDAY TIMES, 16 November 2014, accessed at http://www.thesundaytimes.co.uk/sto/news/focus/article1484299.ece.

[53] Mao Tse-Tung, in Lyman Van Slyke, ENEMIES AND FRIENDS: THE UNITED FRONT IN CHINESE COMMUNIST HISTORY, Stanford University Press, 1967, 168

[54] Introduced by Hendricus Sneevliet, a Dutch Comintern agent operating first in Indonesia, and then in China's Eastern coastal cities.

[55] Lyman Van Slyke, *supra* note 53 at 15.

[56] *Id*.

[57] Mao Tse-Tung, in *Id* at 168.

with the KMT! Instead, recognizing the CCP was better served for the moment by "uniting" with the KMT against the Japanese, Mao and his comrades placed the CCP in a position from which it could survive and build capacity for a future day, while still reserving the option to re-draw the boundaries that separated friend and foe.

This was exactly what occurred in 1945 when, following Japan's surrender, the CCP re-drew a boundary which still (at least nominally) included the KMT as allies, but posited the nebulous presence of elements that sought to perpetuate a civil war within China as the new enemy, in the knowledge that the US (at the time, a power the CCP sought to co-opt or at least neutralize) feared just such a civil war. Within a few months, the line was shifted again, as goals of "peace" and "unity" rapidly morphed into calls for "an anti-feudal united front" (language that both conformed to the rejection of dynastic legitimacy that underpinned both KMT and CCP platforms, while also subtly playing to more radical Communist concepts,) then ultimately into the existential need for an "anti-Chiang [Kai Shek, the KMT leader] united front."[58] I believe this meme evolution suggests United Front Theory guided a deliberate CCP information strategy to:

1. Present the CCP in a favorable light to both extant allies and potentially undecided parties
2. Co-opt potential resources of an opponent by actively and selectively framing the debate
3. Define, isolate, and ultimately destroy legitimacy of a specific, manageable subset of opponents

In other words, United Front Theory served the CCP as a Netwar management tool, allowing identification of potential *conceptual boundaries* that could be promulgated to isolate a specific subset of an adversary, while simultaneously framing the public debate in terms that deterred the target's potential allies from associating with it.

United Front Theory is based upon Marxist dialectics and theories of "contradiction," and as refined by Mao, posits the presence of both a principle contradiction and many lesser contradictions at any given moment. The principle contradiction cannot be resolved without struggle, and is thus deemed to be an "antagonistic" contradiction. Many lesser, "non-antagonistic" contradictions also exist, but can be put on hold until the initial "antagonistic" contradiction is resolved, and any third parties with whom a "non-antagonistic" contradiction exists may be dynamically co-opted within the United Front to facilitate resolution of the "antagonistic" contradiction. However, upon resolution of the primary "antagonistic" contradiction, by definition a new "antagonistic" contradiction will evolve to take the primary place. Thus at all times there is a core protagonist group, a "wavering" middle that may split either way, and an existential foe who must be destroyed or transformed into a non-contradictory entity.[59]

The art of executing United Front Theory is to reduce to the absolute minimum the boundaries of the entity deemed to be in "antagonistic contradiction" (thus allowing the most concentrated and efficient application of resources against it,) to co-opt (or deter from participation) the broadest possible swath of the "wavering" middle (thereby eliminating them as an adversary resource, and possibly leveraging them as a supporting resource,) and to anticipate, and stand

[58] *Id*. at 188-189.
[59] *Id*. at 249-251.

ready to re-draw, the new boundaries of contradiction as the strategic environment evolves (an opponent may also be seeking to do the same, and the new psycho-structural features, once established, may require significant effort to erode.) Mao and the CCP historically executed this evolution in fast geopolitical time, sometimes acting within days. In a modern age of targeted political messaging,[60] online A-B testing (the presentation of unique versions of a message to different groups within a targeted online audience, in order to measure responses and optimize desired effect,)[61] and near-real-time semantic analysis,[62] [63] United Front Theory can operate at netspeed.

7. LEGAL WARFARE

At this point it is worth noting that while information and sentiment may move at netspeed, their lumbering, normative counterparts - policy and law – still do not, and in the space between these two worlds, China has developed another facet of Netwar, "Legal Warfare" (or what Major General Charles Dunlap, Jr. has called "Lawfare."[64]) The leading western scholar of Chinese Legal Warfare, Dr. Dean Cheng, suggests that Legal Warfare illustrates a broader Chinese effort to expand conflict beyond the military domain.[65] One of "three [non-traditional] warfares" articulated in doctrinal writings by the modern Chinese state,[66] conduct of Legal Warfare accelerated in December of 2003 when policy – specifically, revised Political Work Regulations of the Chinese People's Liberation Army – directed the General Political Department (GPD) of the PLA to undertake "three warfares" as part of its implementation of political work.[67]

Operating in synergistic concert with the other two "warfares," psychological warfare (defined as fairly standard 'will-eroding' activities,) and public opinion/media warfare (*"…a constant, ongoing activity, aimed at long-term influence of perceptions and attitudes [via domestic and foreign] news media…movies, television programs, and books,"*) the function of Legal Warfare is to inculcate *"…doubts among adversary and neutral military and civilian authorities, as well as the broader population, about the legality of adversary actions, thereby diminishing political will and support and potentially retarding military activity."*[68]

Here one can see the potential intersection between Legal Warfare, as a *component* of Chinese Netwar, and United Front Theory, as a guiding *framework* for Chinese Netwar. Taking the PLA/GPD as our protagonist, the "antagonistic contradiction" can be defined as an undesired legal,

[60] Kate Kaye, *Post Election, Campaigns Try to Link Targeted Ads to Actual Votes - Here's How Political Groups Know When Digital Ads Drove Voters to the Polls*, AdAge, 24 November, 2014, accessed at http://adage.com/article/datadriven-marketing/political-campaigns-link-voter-aimed-ads-actual-votes/295936/.

[61] Brian Christian, *The A/B Test: Inside the Technology That's Changing the Rules of Business*, WIRED online, 25 April 2012, accessed at http://www.wired.com/2012/04/ff_abtesting/.

[62] Seth Grimes, *What are the most powerful open-source sentiment-analysis tools?* 8 January 2012, Breakthrough Analysis, accessed at http://breakthroughanalysis.com/2012/01/08/what-are-the-most-powerful-open-source-sentiment-analysis-tools/.

[63] 2014 Sentiment Analysis Symposium, accessed at http://sentimentsymposium.com/.

[64] Major General Charles J. Dunlap, Jr., USAF, *Lawfare Today: A Perspective*, YALE JOURNAL OF INTERNATIONAL AFFAIRS, Winter 2008, 146.

[65] Dean Cheng, *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response*, 26 November 2012, accessed at http://www.heritage.org/research/reports/2012/11/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-american-response.

[66] *Id.*

[67] *Id.*

[68] *Id.*

normative, or military activity undertaken or advocated by an adversary; and the "wavering" middle ground can be seen as all those "adversary and neutral military and civilian authorities, as well as the broader population" that may be swayed. The PLA operational objective is thus the *effect* of reducing opponent "…political will and support and potentially retarding military activity,"[69] achieved via a synergistic execution of Legal Warfare, psychological warfare, and public opinion/media warfare.

Dunlap notes, "information technologies have … vastly increased the scope, velocity, and effectiveness of such [Lawfare] efforts,"[70] and one need only look to Chinese online press to find candidate examples of United Front Netwar addressing legal disputes. For example, in the 2012 Xinhua article titled *"China's blueprint means opportunities, not threats,"* Chinese state media simultaneously suggested opposition to China in the legal domain would bring economic ruin, stoked regional fear of western decline and abandonment, and deterred "internationalizing" of legal disputes, arguing that "cementing economic bonds within Asia remains key to the region's continuous growth, as the eurozone sovereign debt woes are far from over, with a fiscal cliff threatening a fragile recovery in the U.S. economy and protectionism on the rise globally. Internationalizing the South China Sea issue will not help resolve the disputes but can sabotage efforts to carry out friendly negotiations on the issue and hamper much-needed regional economic cooperation."[71]

At first glance this might seem an expedient response to anomalous regional and international conditions, but if Cheng is correct, Legal Warfare (and the Netwar conducted in support) is not viewed by the Chinese as an action to be initiated upon tensions or hostilities, nor, as Dunlap suggests, as part of pre-existent "confines of the law"[72] which a Judge Advocate General (JAG) Officer might help warfighters navigate, but rather a cause to be constantly advanced in parallel with other "phase zero" shaping activities, and represents part of "…*the foundation* … [that] *must be established during peacetime so as to create beneficial conditions and context for the military conflict and, in turn, precipitate an early end to a conflict on terms favorable to the PRC.*"[73]

This suggests both peacetime legal claims, and Chinese contention of foreign legal claims *during* peacetime, should be evaluated not only as expressions of Chinese national interest, but also as both *preparation of* a multidimensional Netwar battlespace, and as a form of Netwar itself. In short, any would-be challengers to Chinese ambition must expect sustained, pre-emptive campaigns to reframe normative, legal, and military issues in ways that paint them as dangerous outliers while embedding Chinese goals within constructs likely to be, or already, embraced by a majority of stakeholders. This is a strategy unlikely to be countered by reactive efforts (which cede to China, or any other Netwar opponent, the ability to set the very boundaries of the front.) Instead, sustained counter-strategies, and analytic entities capable of delivering a thorough analysis of the dynamic normative and psychological terrain that these strategies must operate within, are needed.

[69] *Id.*

[70] Major General Charles J. Dunlap, Jr., *supra* note 64 at 148.

[71] China's blueprint means opportunities, not threats, Xinhua News 22 November 2012, accessed at http://news.xinhuanet.com/english/china/2012-11/22/c_131993006.htm.

[72] Major General Charles J. Dunlap, Jr., supra note 64 at 151.

[73] Dean Cheng, *supra* note 65.

8. A ROLE FOR CYBERDEFENSE ORGANIZATIONS IN NETWAR

"Perhaps the most important future battlefield for psychological warfare, though, is the Internet..."[74]

The principle strengths of free societies may make them inherently more vulnerable to the effects of Netwar. Open 'information borders,' vital to debate and commerce, provide thin protection against tailored deceptions veiled as gossip, market preference, opinion, or social interaction. Yet, *inherent* vulnerability need not equate to *actual* vulnerability. While free nations are rightly reluctant to control or censor any legally conducted expressions of belief, there is no reason they cannot convey findings regarding a foreign influence campaign, the dubious origins of a propagating meme, or objective facts – no matter how uncomfortable a position they paint an offending nation in - to their own population. In fact, given that in the modern age the vast majority of content in a Netwar will at some point transit the Internet, and given that the "networked technology" of that Internet has sovereignty associated with it, one might argue that a truly responsive democracy must be prepared to warn of, and if needed counter, a range of Netwar actions directed at it in a timely and transparent fashion, or else be deemed to have ceded a measure of sovereignty over its own cyberspace.

If this is the case, then the technology and skills of a Cyberdefense organization will have important roles to play. In the civil sector, Cyberdefense traditionally entails heightened, near-real-time situational awareness of internet activity; maintenance and control of backup communication and networking capabilities held in reserve; and established advisory and consulting relationships with subject matter experts and counterpart organizations across industry, academia, and government. All of these tools may be of utility in countering a Netwar campaign.

For example:

1. Cyberdefense organizations could be tasked to identify the emergence of Netwar-associated memes and actions in open online content. To guard against any potential misuse, warning activities could be transparent to the entire population served, and capabilities could remain under both the operational control and oversight of duly elected civilian officials.

2. Cyberdefense tools to characterize quantitative and qualitative shifts in network activity[75] could be called upon to reconstruct, track, and attribute Netwar-associated activities. A nation or alliance's citizens deserve to know if ten-thousand seemingly different online identities, all confirming the "fact" of an occurrence that their own leaders dispute, are in reality merely five persons operating under orders from a basement within an adversarial nation.

3. If and when Netwar is executed in combination with other forms of warfare – either Cyberwar, or kinetic war – Cyberdefense organizations may possess the capacity to counter certain Netwar actions with potentially existential

[74] *Id.*

[75] See for example the Internet Storm Center at www.sans.org , or Google's TRENDS feature at www.google.com.

> consequences. Cyberdefense organizations should be prepared to use any out-of-band communication capabilities, reserve modes, international partnerships, or civil-military-industrial interfaces they possess to enable an authoritative and timely response by their civilian leadership within the information domain.

Moreover, Cyberwar and Netwar have become increasingly intertwined, and the impact of cyber actions can be either potentiated or mitigated by corresponding psychological and normative conditions. Thus, an effective Cyberdefense must also incorporate a set of informed Netwar responses.

9. CONCLUSION

Responding to modern Netwar need *not* require the initiation of a Cyberwar in response, nor a claim in the United Nations Security Council that the threshold of any type of conflict (other than the here-defined concept of Netwar) has been breached. President Putin may express the sentiment that the west is conspiring against Russia[76] without his paranoia constituting a *casus belli*. So too is Minister Baird free to draw attention to ongoing Russian manipulation of information. But the west should not become complicit in affording such different, and differently-intentioned, statements conceptual equality on a national, regional, or global, media stage, nor should western decision-makers cling to the hope that Netwar opponents will refrain from elevating their own voices at the expense of truth, either overtly or through a façade of intermediaries.

Fortunately, the antidote to Netwar poison is active transparency, a function democracies excel in. A United Front, as it were, of truth-seeking nations, soberly facing their opponents, willing to accept the airing of one's own imperfection for the sake of improvement, and committed to the norm that there is an objective reality that matters, presents a formidable challenge to the information-machinations of undemocratic or authoritarian regimes. There is no reason the west cannot accept the insights in these eastern perspectives, and we should apply them, leveraging both new mechanisms and extant Cyberdefense organizations, within a morally appropriate Netwar framework, to advance our shared interests on the global stage.

[76] Mark Franchetti, Toby Harnden and Michael Sheridan, *supra* note 52.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Russian Information Warfare of 2014

Margarita Jaitner
Department of Military Studies
Swedish Defence University
Stockholm, Sweden
Margarita.jaitner@fhs.se

Dr. Peter A. Mattsson
Department of Military Studies
Swedish Defence University
Stockholm, Sweden
peter.mattsson@fhs.se

Abstract: The belief in the power of information is deeply ingrained in the minds of the Russian top leadership, which operates under the premise that public opinion can be effectively influenced in order to reach desired outcomes domestically as well as on foreign soil. Ever since the beginning of the Euromaidan demonstrations, Russia has been seeking to promote its own narrative domestically, in Ukraine, and beyond, making use of the unique features of the cyberspace. As the crisis deepened in early spring of 2014, information operations played an important role in facilitating the de facto annexation of the Crimean peninsula to the Russian Federation, as well as throughout the continuation of the crisis.

This paper sets out to examine the information-related events of early 2014 with a particular focus on the annexation of Crimea. The aim is twofold. First, it provides an insight into the Russian world of ideas regarding information and its power applying the concept of information superiority and how it connects cyber and information warfare. Second, this paper exemplifies how Russia or pro-Russian entities make use of a wide array of tools and methods – kinetic, cyber, and informational – with the purpose of achieving information superiority. The paper concludes with a discussion regarding the impact of cyber within Russian Information Warfare as experienced in Ukraine.

Keywords: *information operations, information warfare, cyberspace, social media, Russia, Ukraine*

1. INTRODUCTION

"All warfare is based on deception," wrote Sun Tzu in "The Art of War". Information and communication have always played a role in conflict: ever since antiquity, symbols, rhetoric, and (mis)information have been used to gain advantage by frightening and misleading the enemy. Knowledge of the opponent's plans and capabilities, on the other hand, has the potential to balance differences between the combatants' firepower, contributing to victories. Russia has a long history of using misinformation and misdirection in conflict to create benefits for domestic and foreign policy (Glantz 1988) as well as of using agitation and propaganda to mobilize its population (Kenetz 1985). Therefore, it is hardly surprising that the country's current leadership seeks to exploit the new complex networked information environment to its advantage. When the Ukraine crisis came to its first peak with the annexation of the Crimean peninsula, it became clear that Russia was conducting intense Information Operations (IOs), and, more so, that it was yielding success with these. The Information Warfare (IW) as such, however, had begun much earlier and gained intensity ever since the first Euromaidan demonstration.

IOs exist in a direct context with other types of operations such as military action, as experienced throughout the crisis in the Ukraine. In this light, the relatively bloodless but disinformation-rich annexation of Crimea must be seen as an absolute success. Still, because of the diffuse nature, it is difficult to estimate the exact impact of IOs. While areas with more exposure to other-than-Russian narratives are likely to be more resilient to Russian IOs, it is safe to say that Russia will continue to make use of its IW capabilities and that these are likely to have an impact on physical events. The present article aims to provide an overview over Russian application of IO/IW during the 2014 crisis in Ukraine and, to the extent it is possible, identify what contributes to their success. An essential element herein is to describe how information warfare converges with other types of warfare, in particular with cyber. The article is limited to cover pro-Russian activities during 2014; however, referenced to past events are made when deemed necessary. While examples of IOs against other countries are used, the paper's focus is on Ukraine.

2. INFORMATION AND CYBER SECURITY IN RUSSIAN (MILITARY) THEORY

The Russian policy and academic view on information as a source of power provides important background for the country's conduct of IOs. Russian focus on information and "information superiority" ("информационное превосходство") is an important element in the country's doctrines and strategies. The "National Security Strategy 2020" (Security Council of the Russian Federation 2009), for example, states in its analysis of future threats that the "global information struggle will intensify". In the same context, "nationalist, separatist, radical religion" and another agitation is deemed to become a danger to the Russian state. The strategy proposes to counter these threats by disseminating "truthful" information to citizens as well as promoting development of native platforms – such as own social media. Other official documents, such as the Information Security Doctrine of the Russian Federation (Security Council of the Russian Federation 2000), the Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (Ministry of Defence of the Russian Federation 2011) as well as the Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (Security Council of the Russian Federation 2013), treat Computer Network Operations as an inherent part of information security without distinction. This is also evident in the terminology used in Russian strategies, doctrines. Instead of the Western "cyber security", "information security" ("информационная безопасность") is central. Thus, the Russian perspective cares not only about the technical wholeness of information but also about the cognitive wholeness of information. Message –

towards the state, its executives and the population – can be the gunpowder in the cyberspace. Furthermore, there is also a strong perception of Russia already being the target of an ongoing IW, which is to a significant part waged in the cyberspace (Panarin 2012, 2014a). Hence, the desire to define and safeguard the borders of the Russian "information environment" or "information space" ("информационное пространство") appears to be a logical consequence. Russia is well aware of the discrepancies in the use of terminology, which is evident in the publicly available draft of the Cyber Security Strategy of the Russian Federation (Russian Federation Security Council 2014).

Similarly, the academic discourse grants a lot of focus to information. "Information has become a weapon. It is not just an addition to firepower, attack, manoeuvre, but transforms and unites all of these," say Ivan Vorobyev and Valery Kiselyov (2013) in an academic article on Russian military theory. Sergei Chekinov and Sergei Bogdanov (2011) ascribe even more power to information: "Today, the means of information influence reached such perfection that they can tackle strategic tasks." At the same time, other scholars are trying to make sense of the Western views on cyber and struggling towards an adequate terminology, which would be necessary to counter foreign developments (Balybin, Donskov & Boyko 2014). Still, it seems fairly unlikely that the technical aspects of cyberspace will be divided from the message anytime soon.

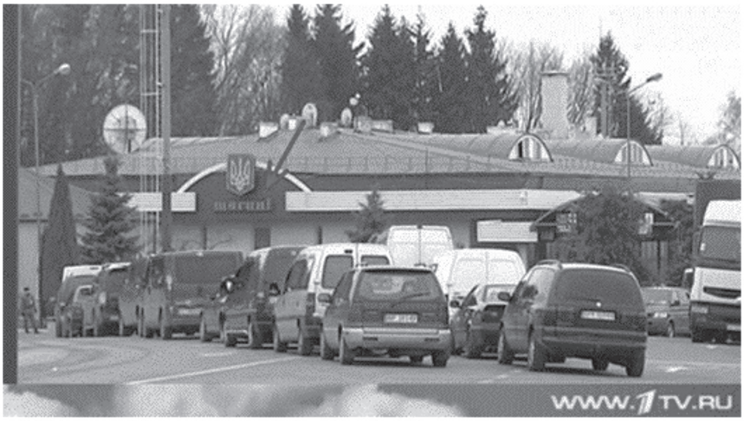
The potential power of information is firmly rooted in the Russian military and political thinking. More so, Russia also considers itself to be a target of ongoing IW: Russian academic literature makes clear that there is a perception of a rift between Russia, or the "historical Russian world", of which Ukraine is part, and "the West" with the US as the principle antagonist. This rift is both ideological and cultural, signified by an incompatibility of values ("духовные ценности") (Putin 2013a, 2013b). It is also perceived that the US continuously conducts IOs against other countries. The revolutions of recent years, such as the Arab Spring, are then explained with such operations. Professor Igor Panarin's (2014) book "Information Warfare and Communications" ("Информационная война и коммуникации") provides an example for this line of thought. The fall of the Soviet Union is a result of what Panarin calls the "first information war". According to him, the US currently engages in a "second information war" against, amongst others, Russia and Syria, to which the five-day war in Georgia in August 2008 was the clearest prelude. Further, Panarin speculates about the existence of an "Operation ANTI-PUTIN", which he compares to "Operation ANTI-STALIN" which was allegedly central to the "first information war". Panarin (2014b) also believes that Wikileaks' Julian Assange is an agent of the British MI-6 and that Euromaidan is the result of Western IOs. The focus on information and its power is not new, but a relic of the Soviet era (Glantz, 1988). In today's networked world, however, there are many more means to disseminate information than ever before.

3. BATTLESPACE (SOCIAL) MEDIA

In recent years, the Russian media landscape has changed significantly. As Freedom House (2014) noted, press freedom declined since Putin was re-elected as president in 2012. Relatively few media outlets feature critical political debate and Kremlin controls many news outlets, either through state-owned companies or aligned business owners. With the advancement of technological development, traditional media sought to extend to new communications platforms. Many large and a high number of small newspapers, radio and TV channels are today present on the web. The step into the cyberspace also paved the way for the media to reach out to the world. Media outlets like RIA Novosti provide versions in English and other languages in addition to Russian-language content. Further, purely externally focusing media such as RT have gained audience abroad. RT is deeply integrated with social media through direct interfaces, the communication possibilities in the comment field. Similarly, the newest Russian media project, Sputnik, seems to be well integrated technically. According to the head of Rossiya Segodnya, Dmitry Kiselyov (2014), Sputnik was created by the Russian government to counter "propaganda promoting a unipolar world".

The Kremlin-aligned Russian traditional media has ever since the beginning of the crisis painted a negative picture of Euromaidan and Kiev. For example, Russian media claimed that hundreds of refugees were leaving Ukraine to seek asylum in Russia as a result of Ukrainian brutality towards the (Russian-speaking) population (TASS 2014a, 2014b, 2014c). In several cases, these reports were accompanied by photo and video material from the Ukrainian-Polish, not the Ukrainian-Russian border (Figure 1). Among other inaccuracies, there were also claims that the Ukrainian Navy frigate Hetman Sahaydachniy defected. Upon refutation, Russian media merely reported that the frigate had loaded NATO intelligence equipment (Sivkova 2014, TASS 2014d).

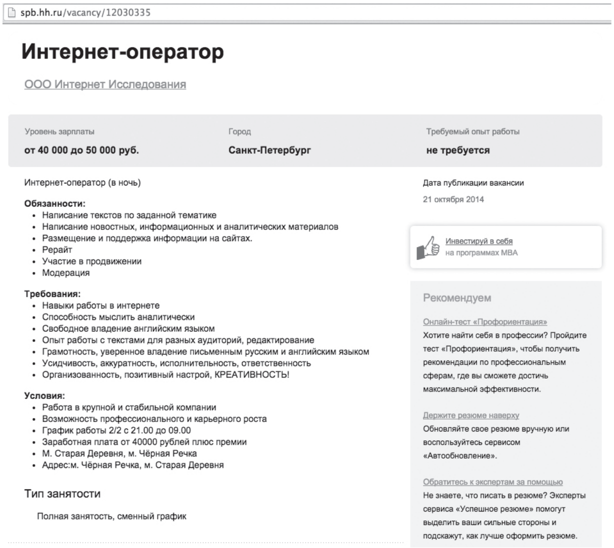
FIGURE 1: RUSSIAN CHANNEL 1 REPORTS ABOUT MASSES OF UKRAINIAN REFUGEES TRYING TO CROSS THE BORDER TO RUSSIA, SHOWING VIDEO FOOTAGE FROM BORDER CHECKPOINT BETWEEN UKRAINE AND POLAND (UMANEC 2014).



Social media constitutes an integral part of the Russian media landscape. In this context, the term "Runet" is interesting. Summing up the entirety of Russian-language content, this term describes the interconnectedness of the various parts. This includes pages that are maintained in Russia as well as pages operated by Russian-speakers abroad, traditional and new media, and other types of pages. All of these constitute nodes in a single large network. The phrase "in the Runet" ("в Рунете") describes how information migrates between different nodes. The term can also gain significance in the light of the Russian desire to define and defend "Russian information space". Seddon (2014) describes the Russian government's approach to the Internet and social media as filled with fear towards an environment that is outside of control.

Since the early 2000s, the Internet has provided a space for political blogs, groups, and forums of varying ideology (Polyanskaya, Krivov & Lomko 2003). Social media was a key driver during the 2011/2012 demonstrations against the re-elections of Edinaya Rossiya and Vladimir Putin. During these demonstrations, pro-Kremlin online groups engaged in political debate, but also worked intensely to discredit the opposition and even to disrupt the organization of anti-government protests (Jaitner 2013). The opposition coined the term "Kremlin's trolls" to describe these groups. It has long been speculated that Kremlin itself employs and pays these "trolls" to spread pro-government discourse and to disrupt the opposition (Polyanskaya, Krivov & Lomko 2003, 2009; Fitzpatrick 2014). In 2014, the Finnish Defence Forces Research Institute confirmed the existence of paid "internet trolls", pointing at a St. Petersburg based company (Myös 2014). At the time of writing, this company continues to recruit employees to "work with social media" (Figure 2).

FIGURE 2: LLC "INTERNET RESEARCH" LOOKING TO HIRE AN "INTERNET OPERATOR". DUTIES: WRITING POSTINGS FOR SOCIAL MEDIA ON A DESIGNATED TOPIC. KNOWLEDGE OF ENGLISH LANGUAGE AND THE INTERNET, AS WELL AS CREATIVITY AND ABILITY TO THINK ANALYTICALLY ARE REQUIRED (HEADHUNTER.RU 2014).



spb.hh.ru/vacancy/12030335

Интернет-оператор

ООО Интернет Исследования

Уровень зарплаты	Город	Требуемый опыт работы
от 40 000 до 50 000 руб.	Санкт-Петербург	не требуется

Интернет-оператор (в ночь)

Обязанности:
- Написание текстов по заданной тематике
- Написание новостных, информационных и аналитических материалов
- Размещение и поддержка информации на сайтах.
- Рерайт
- Участие в продвижении
- Модерация

Требования:
- Навыки работы в интернете
- Способность мыслить аналитически
- Свободное владение английским языком
- Опыт работы с текстами для разных аудиторий, редактирование
- Грамотность, уверенное владение письменным русским и английским языком
- Усидчивость, аккуратность, исполнительность, ответственность
- Организованность, позитивный настрой, КРЕАТИВНОСТЬ!

Условия:
- Работа в крупной и стабильной компании
- Возможность профессионального и карьерного роста
- График работы 2/2 с 21.00 до 09.00
- Заработная плата от 40000 рублей плюс премии
- М. Старая Деревня, м. Чёрная Речка
- Адрес:м. Чёрная Речка, м. Старая Деревня

Тип занятости

Полная занятость, сменный график

Дата публикации вакансии

21 октября 2014

Инвестируй в себя
на программах MBA

Рекомендуем

Онлайн-тест «Профориентация»
Хотите найти себя в профессии? Пройдите тест «Профориентация», чтобы получить рекомендации по профессиональным сферам, где вы сможете достичь максимальной эффективности.

Держите резюме наверху
Обновляйте свое резюме вручную или воспользуйтесь сервисом «Автообновление».

Обратитесь к экспертам за помощью
Не знаете, что писать в резюме? Эксперты сервиса «Успешное резюме» помогут выделить ваши сильные стороны и подскажут, как лучше оформить резюме.

Interestingly, some of the social media accounts that can be linked to use by trolls have been created long in advance while the first activity of these Internet personas was recorded during the crisis. According to the "hacktivist" group "Anonymous", up to 600 paid "trolls" work in St. Petersburg (Baltic News Network 2014).

The troll activity is not limited to Runet with intense pro-Russian discourse appearing in commentaries on Western traditional and social media (Sindelar 2014). The Baltic countries see themselves as particularly vulnerable: paid "Kremlin-trolls" are working not only from St. Petersburg but also in Estonia and Latvia (Baltic News Network 2014; The Lithuanian Tribune 2014).

Ukraine, with its large Russian speaking population, has long been an integral part of the Russian traditional and social media's audience. It is difficult to draw a definitive line between Runet and Ukrainian-language Internet. For example, before the crisis took place, the Russian equivalent of Facebook, VKontakte, was the most popular social media site amongst Ukrainian users. Another favourite social media is Odnoklassniki, or "Classmates" (ok.ru, 2014), where roughly 20 million profiles claim that they reside in Ukraine. However, the use of Russia-associated social media declined since the beginning of the crisis in favour of the Western alternative, Facebook (Unian 2014). Still, a mix of Russian and Ukrainian languages, as well as attitudes, is observable in political and other discussions throughout the social media. Antimaidan-discourse has been persistent throughout the crisis (Security Service of Ukraine 2015). The topics in this discourse correspond largely with the reporting in traditional Kremlin-leaning media. Herein, significant attention is given to nationalist and fascist participation in Euromaidan demonstrations (Anpilov 2013, RIANovosti 2014a, 2014b). Unsurprisingly, potential threats to "ethnic Russians" and the status of the Russian language are hot topics. These were fuelled by the attempt to amend Ukraine's legislation in the latter matter shortly after the interim government was installed. Although the bill was unsuccessful, it provided the pro-Kremlin debaters with "sufficient evidence" for hostility towards the Russian-speaking minority.

4. CASE CRIMEA AND NOVOROSSIYA[1]

When uniformed, armed individuals wearing no insignia appeared on the Crimean peninsula and later also in eastern Ukraine, Russian-leaning media nicknamed them "friendly people" who were "good to civilians" (Leonov 2014). The Ukrainian side called them "little green men", immediately identifying them as troops under Russian order. For weeks, Vladimir Putin (2014b) denied the participation of Russian troops in the Crimea take over and Defense Minister Sergei Shoigu (2014) called the rumours "nonsense and provocation". Nevertheless, the Russian-language media proceeded to portray these "soldiers of the future" as extremely well equipped and professional (Leonov, 2014). Meanwhile, Ukrainian troops stationed in Crimea were offered to pledge allegiance to the Russian Federation or alternatively to leave the peninsula or resign from their military careers. Russian media was then quick to report about large-scale surrender by Ukrainian troops (Yuzhniy Kurier 2014, CNN 2014). In retrospect, Verhovna Rada member Gennady Moskal (2014) blamed the fact that the Ukrainian troops had not received permission to use their weapons in time. Dmitry Tymchuk (2014) – Ukrainian military commentator and the front figure of the "Information Resistance" group[2], which gained a lot of popularity during the crisis – commented the events by accusing the interim government

[1] Novorossiya – historically a region north of the Black Sea, annexed by the Russian Empire following the Russo-Turkish wars. The term was revived to denote a confederation of the self-proclaimed Donetsk People's Republic and Lugansk People's Republic in eastern Ukraine.

[2] "Information Resistance" is, according to its own description on http://sprotyv.info/en/about-us, a non-governmental project that aims to counteract external threats to the informational space of Ukraine". The group provides operational data and analytics. As one of the project's front figures, Dmitry Tymchuk has provided analysis to, amongst others, Kyiv Post and Huffington Post.

in Kiev of having handled the situation in Crimea slowly and without sufficient clarity. However, the totality of IW in Crimea might have significantly added to Kiev's difficulties getting a clear picture of the events on the ground and thus have slowed down the decision making process.

The events in Crimea that unfolded in spring of 2014 provide important clues for the interplay between IOs and kinetic activity. The course of events – from the takeover of parliament in Simferopol and dismantling of the Ukrainian military presence on the peninsula, to the disputed referendum and the de facto annexation of the area to the Russian Federation – was accompanied by intense activity aimed to control the flow of information. This activity extended across the entire spectrum of communication and included kinetic, cyber and IOs targeting the physical, logical and social layers of communication.

In early March, Ukrtelecom reported kinetically damaged fiber optic cables and a temporary seizure of the company's offices; further disclosures described jammed naval communication (Maurer & Janz 2014). The head of Security Services of Ukraine also confirmed that government officials' mobile communications fell victim to an "IP-telephonic attack" (Paganini 2014). Some argued that attacking Ukrainian telecommunication equipment was a relatively easy task due to similarity to its Russian counterparts (Maurer & Janz 2014). However, this is also likely to be true for other critical infrastructure in the Ukraine. Still, communication channels appeared to be the primary target. In addition, there were reports of Distributed Denial of Service (DDoS) attacks as well as website defacements targeting political, government, and news websites (Maurer & Janz 2014, Pernik 2014). Examining cases of cyber attacks against Ukraine at that time, it quickly becomes evident that publicity was a crucial factor in the selection of possible targets. The "hacktivist" group "CyberBerkut" ("Киберберкут" http://cyber-berkut.org/en) claimed to have attacked the Ukrainian electronic voting system and later to have also successfully defaced several NATO websites (Maurer & Janz 2014, Paganini 2014). While these attacks are technically not very advanced, they suit to make a statement and are difficult to interpret for laymen, as in the case with NATO websites, or to sow distrust in systems, as in the case with the voting system. What is more, such attacks create speculations regarding the attackers' overall capabilities without revealing their full arsenal (Maurer & Janz 2014).

Striving for information superiority also implies the desire to access adversary's information. Cyberberkut repeatedly claimed to have gained access to telephone recordings and e-mail correspondence between Ukrainian, EU, and US officials and disclosed the content. In addition, the SBU (2014) warned that Ukrainian officials are targets of espionage malware distributed via e-mail. The espionage malware "Snake", "Uroboros" or "Turla", discovered in Ukrainian networks and forensically linked to Russia, remained the most advanced cyber activity against Ukraine. While it still largely aims at information, it cannot be linked to the immediate Ukrainian conflict directly because it appears to have been residing in Ukrainian networks since 2010 (Infosecurity Magazine 2014, Symantec 2014).

In many cases, it is difficult to distinguish information (or disinformation) that originates centrally from content that is created and disseminated by individuals based on their own opinion and experience. Throughout the crisis, pro-Russian activists and fighters have created and uploaded videos, photographs as well as written testimonies and continue to do so. Once content is made available online, it is disseminated across various nodes, often taken out of its original context and given a new, sometimes contradictory, meaning by individuals or in an organized manner. Such intense activity naturally helps creating what can be called "the fog of information war", which fosters polarization amongst the spectators, who in turn influence the higher political levels' ability to act.

The importance of information superiority becomes apparent when looking at how much planning and resources were put into creating "official" as well as semi-official "information agencies". Among these are even several YouTube (2014) channels reaching relatively large audiences. Websites related to "Novorossiya" are particularly interesting: novorus.info and novorossia.su were, according to who.is, registered in March 2014. The use of this term, however, was popularized at a later point in time: Putin used the historical concept to describe the southeastern parts of Ukraine for the first time in a live phone-in on April 17, 2014 (Putin 2014a) and the so-called confederation Novorossiya was formally created on May 24, 2014. Similarly, the "official" websites of the People's Republics Donetsk and Lugansk were registered before the entities were self-proclaimed.

Online pro-Russian content also fills another auxiliary function: recruitment of combatants as well as supporting supply and logistics. This includes calls for monetary donations, necessities for children, medical supplies as well as practical information for those willing to travel to combat zones. Activists of extremely varying ideologies recruit combatants to join the rebel forces in eastern Ukraine. An interesting observation in this context is how various ideologies converge for a "universal goal". For example, a thread on a Stalinist forum ("17th of March Movement" or "Общесоюзное движение 17 марта" 2014) features recruitment information provided by imperialists, communists, nationalists as well as "orthodox patriots". Even volunteers from the North Caucasus have found their way to the conflict – video clips on various social media testify Kadyrov's followers' ("Кадыровцы") involvement in the fighting in eastern Ukraine. The individual posts differ rhetorically. Based on on a common slim narrative, different elements characterize the evilness of the foe with a common denominator: a fight for the "good" values and fraternity with the people of eastern Ukraine. Depending on the individual ideology, activists use communist slogans, prayers and "Russian-orthodox" values as well as grave anti-Semitic speech. While the various groups' discourse differs significantly, the lowest common denominator appears to be the mention of fascism as a foe. Given the constantly upheld memory of the Great Patriotic War, this is hardly surprising – even though the term is interpreted differently within the individual groups. Another notable factor is that, despite the convergence, there is little evidence for hostility between groups of conflicting ideology – a common foe unites.

5. THE ANATOMY OF RUSSIAN INFORMATION WARFARE

Ever since the dawn of the Ukraine crisis, the physical events were accompanied by an intense information struggle, a struggle to establish a narrative but also to mislead the opponents. Despite its likely origin at the top political level, this struggle differs from the pre-Internet and pre-globalization propaganda in some important aspects. Unlike propaganda during Soviet times, which relied heavily on narratives designed at the top level as well as on isolation, today's Russian IW incorporates the audience as a narrative-bearing and a narrative-developing factor. Furthermore, today's countless interfaces between various audiences – such as domestic, diaspora, and foreign – present a probably insurmountable obstacle for conveying individual narratives to different audiences. Therefore, anything that the top leadership aims to share with domestic audience is almost instantly shared with the foreign population. This creates a requirement to tailor narratives to fit a large audience.

The interplay between different levels of information – from the political leadership of President Putin at the tip, via the traditional media to the grassroots level in social media – appears to be an important core element of the Russian IW. One of the core narratives surrounds Russia's position in the world: a misunderstood counterweight to Western liberal values and a misjudged historic superpower. This narrative is slim and can be easily absorbed by the general population and even groups abroad. Being slim and universal, this narrative provides a perspective or a foundation for interpretation of further events. Once it reaches the grassroots level, it can be customized to fit various groups' individual ideologies. Elements can be highlighted or refilled with attributes in accordance with a group's opinions – by the group itself. For example, nationalist groups focus on Russia's historical position of power, while communist groups discuss Russian antagonism to capitalism with reference to the Soviet era. Applying such pyramid method has at least two advantages. First, since individual flavours of narratives are created at group level, their competition is less exposed to the general public. Second, there is no need to design individual narratives and inject these into groups. Instead, already existing group dynamic is utilized, including the group's opinion-makers' position of trust within the group.

Because the narrative at its origin aims at both domestic as well as foreign audience, the mechanism also serves its purpose outside the country. The idea of a "Russian World" ("Русский Мир") as the bearer of "Russian soul" and "Russian values", which does not only include ethnic Russians but the world's "Russian-speaking population", is continuously maintained and serves as a unifying factor. In extension, the message is also transported beyond the Russian-speaking diaspora. The narrative for the world outside Russia and former Soviet area is complemented by information that aims to seed doubts and distrust towards the Western systems. Western "hypocritical behaviour" and "decay of traditional values" are two of the frequently recurring topics, which particularly gain attention within system-critical groups.

A particular focus on the grassroots level is detectable, evident by the use of "trolls" or "opinion agents". Such practice indicates an inherent understanding of how to penetrate societies that are naturally sceptic towards mainstream information channels. It also implies an awareness of the importance of popular opinion, as well as an understanding of the significance of "private" or interpersonal channels of communication. In the post-Soviet environment where the population has little trust in official information, interpersonal communication gains importance. Information shared by an acquaintance enjoys more trust than the message provided through media (Lonkila 2012). Meanwhile, in open societies, this methodology can successfully create doubts in regard to objectivity that is desired from the mainstream media. Due to the relative anonymity in the cyberspace, trolls can operate by blending into the crowd, being difficult to detect by laymen. Similarly, cyber events of little technical harm, such as DDoS, website defacements, or mere suggestion that a system has been compromised by an intrusion, can present themselves as far more impactful to laymen. This in turn sows distrust in established systems, especially when paired with efforts to create an informational blackout, as seen in Crimea. The (partial) blackout itself then hinders the attacked side to gain an overview of events and, at the same time, allows the attacking side to promote its own narrative.

Inside the Russian sphere of influence, the younger generation that grew up in the post-Soviet era is seen as a weak link, evident through concern with the youth being receptive to undesired influences (Putin 2014c). Having inherited their parents' distrust in mainstream media, they also enjoy a greater access to non-Russian content and thus are, according to Kremlin's line of thought, exposed to influence from the West. At the same time, it is possible to reach the younger generation via social media in urban centres, where both Internet penetration and affiliation with Western values are high. Russian IW strategists likely see these areas as most problematic. A certain level of criticism and counter-narrative may be desired to be able to relate propagated narrative to an antithesis, and to maintain an illusion of freedom. The impact of IW at the grassroots aiming on the younger population in urban centres in post-Soviet countries appears to be a particularly interesting subject to scrutinize in detail, possibly in the context of vulnerability of open societies in general.

6. CONCLUSIONS: THE ROLE OF CYBER IN RUSSIAN IW

Technological developments of the recent decades have presented new possibilities to enhance and expand IW geographically, while also presenting those who want to engage in IW activities with new challenges. Russian leadership appears to have adapted to the new, networked environment, putting a large focus on efforts throughout the crisis on information and control thereof. Here, physical efforts converge with cyber attacks and other influence activities. Particularly during the seizure of Crimea a twofold use of cyber could be observed: attacks against telecommunication equipment and media channels appear to have contributed to a communication blackout, while other attacks aimed at influencing the opinion of domestic and foreign audiences. In this context, technically less advanced attacks, such as DDoS or website defacements can be argued to constitute a part of cyber IW. Also, while the Uroboros spyware cannot be absolutely attributed to the particular crisis, it is an instrument for gaining information superiority. In this perspective, cyber has contributed to the course of the events as a part of overall IW efforts. Meanwhile, the cyberspace as such has required adaptation in Russian IW practices. Probably most obvious adaptations are the use of a slim narrative and the utilization of "trolls" who thrive in an environment of relative anonymity. Furthermore, the networked reality enhances the influence-bearing factor of any action, such as the deployment of troops. Russian IW seeks to utilize these factors by providing a narrative as a base for interpretation of events.

Overall, IW has significantly contributed to the successful annexation of Crimea, as well as to the creation of the Novorossiya concept and thus to the continuation of the crisis. This in turn highlights the need to address the new ways IW is conducted. The convergence between malicious cyber activities and IW deserve professional and policy attention. What might be called conventional cyber attacks by Russia were almost negligible; however, these new cyber aspects must be considered as an integral part of new information warfare.

REFERENCES

Anpilov, V. 2013. “Анпилов: Фашисты захватывают Майдан. (Anpilov: Fascists taking over Maidan.)” *Pravda*. Accessed 10 December 2014. http://www.pravda.ru/world/formerussr/ukraine/10-12-2013/1184934-anpilov-0/

Baltic News Network. 2014. “Latvia overrun by Kremlin-financed internet trolls.” *Delphi by The Lithuanian Tribune*, 4 December 2014. Accessed 20 December 2014. http://en.delfi.lt/nordic-baltic/latvia-overrun-by-kremlin-financed-internet-trolls.d?id=66577080

Balybin, C. Donskov, Yu. and Boyko A. 2014. “Electronic Warfare Terminology in the Context of Information Operations.” *Military Thought* 23 (3).

Checkinov, S. & Bogdanov S. 2010. “Asymmetrical Actions to Maintain Russia’s Military Security.” *Military Thought* 2010 (1).

CNN. “CNN: Украинские войска в Крыму сдаются силам самообороны. (Ukrainian troops surrender to Crimean self-defence forces.)” *edited by RT*, 19 March 2014. Accessed 17 December 2014. http://russian.rt.com/inotv/2014-03-19/CNN-Ukrainskie-vojska-v-Krimu

Fitzpatrick, C. 2014. “Russia This Week: The Kremlin’s Growing Army of Internet Trolls.” *The Interpreter*, 14 November 2014. Accessed 21 November 2014. http://www.interpretermag.com/russia-this-week-the-kremlins-growing-army-of-internet-trolls/

Freedom House. 2014. Russia. Freedom of press 2013, 2014. *Freedom House*. https://www.freedomhouse.org/report/freedom-press/2013/russia - .VH74sJPF800:

Glantz, D. 1988. “Surprise and Maskirovka in Contemporary War.” *Army Combined Arms Center Fort Leavenworth KS Soviet Army Studies Office*. Accessed 13 November 2014. http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA216491

Headhunter.ru. 2014. ”Интернет Оператор. (Internet Operator.)” *HeadHunter.ru.* Accessed 17 November 2014. http://spb.hh.ru/vacancy/12030335

InfoSecurity, Magazine. 2014. “Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia.” *InfoSecurity Magazine*, 11 March 2014. http://www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/

Jaitner, M. 2013. “Exercising Power in Social Media.” *The fog of cyber defence*., edited by J. Rantapelkonen, & Salminen, M. Julkaisusarja 2. Artikkelikokoelma no: 10.

Kenez, P. 1985. *The birth of the propaganda state: Soviet methods of mass mobilization, 1917-1929*. : Cambridge University Press.

Kiselyov, D. 2014. Дмитрий Киселёв представил международный проект “Спутник”. (Dmitri Kiselyov introduces the international project “Sputnik”.) *YouTube.* Accessed: 20 December 2014. https://www.youtube.com/watch?v=WR6qEi8I-IE

Leonov, A. 2014. “Солдаты будущего: чем вооружены «вежливые люди» в Крыму. (Future soldiers: The friendly men’s equipment in Crimea.)” *Forbes,* 7 March 2014. Accessed 20 December 2014. http://m.forbes.ru/article.php?id=251676

Lonkila, M. 2012. “Russian Protest On-and Offline: The role of social media in the Moscow opposition demonstrations in December 2011.” *UPI FIIA Briefing Papers* 98 (2012).

Maurer, T. & Janz, S. 2014. “The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.“ *The International Relations and Security Network*, 17 October 2014. Accessed 14 December 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345

Ministry of Defence of the Russian Federation. 2011. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space.)

Paganini, P. 2014. “Crimea – The Russian Cyber Strategy to Hit Ukraine.” *InfoSec Institute*, 11 March 2014. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/

Panarin, I. 2012. “О Доктрине информационного противоборства России. (On the Russian doctrine of Information Defence.)” *Voyennoye Obozreniye*, 18 July 2012. Accessed 10 December 2014. http://topwar.ru/16540-o-doktrine-informacionnogo-protivoborstva-rossii.html

Panarin, I. 2014a. *Информационная война и коммуникации. (Information warfare and communications.)* Moskva, Russia: Goryachaya Liniya - Telekom.

Panarin, I. 2014b. Posting on Facebook, 29 June 2014. Accessed 19 December 2014. http://www.facebook.com/permalink.php?story_fbid=487886764691548&id=100004106865632&fref=ts

Pernik, P. 2014. “Is All Quiet on the Cyber Front in the Ukrainian crisis?” *RKK ICDS International Centre for Defence and Security*, 7 March 2014. http://www.icds.ee/et/blogi/artikkel/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis/

Polyanskaya, A., Krivov A. & Lomko I. 2003. “Виртуальное око старшего брата. (Big Brother’s virtual eye.)” *Zhurnal Vestnik*, 3 April 2003.

Polyanskaya, A., Krivov A. & Lomko I. 2009. “The Kremlin’s Virtual Squad.” *Open Democracy*, 19 March 2009.

Putin, V. 2013a. “Путин защитит традиционные семейные ценности. (Putin to defend traditional family values.)” *Vesti*, 12 December 2013. Accessed 20 December 2014. http://www.vesti.ru/doc.html?id=1166423

Putin, V. 2013b. “Наши духовные ценности делают нас единым народом (Our values unite us as peoples.)” Speech in Kiev 27 June 2013.” *YouTube*. Accessed 20 December 2014. https://www.youtube.com/watch?v=YW1WYh_gvJg

Putin, V. 2014a. Прямая линия с Владимиром Путиным. Phone-in with Vladimir Putin. (Transcript). 17 April 2014. Accessed 15 December 2014. http://kremlin.ru/news/20796

Putin, V. 2014b. Путин: “В Крыму нет российских солдат. Это самооборона Крыма. (Putin: There are no Russian soldiers. This is Crimeas popular defense.)” *YouTube*. Accessed 20 December 2014. https://www.youtube.com/watch?v=qzKm7uxK8ws

Putin, V. 2014c Security Council meeting 20 November 2014. Transcript. Accessed 21 November 2014. http://kremlin.ru/news/47045

RIANovosti. 2014a. “ ‘Фашисты’ и ‘террористы’: СМИ США выясняют, кто есть кто на Украине. (‘Fascists’ and ‘terrorists’ Media in the US sorts out who is who in the Ukraine.)” *RIA Novosti*, 18 May 2014. Accessed 20. December 2014. http://ria.ru/world/20140518/1008297621.html

RIANovosti. 2014b. “Более 140 тысяч граждан уехали из Украины в Россию, заявил сенатор. (Senator: More than 140k Ukrainians left for Russia.)” *RIA Novosti*, 1 March 2014. Accessed 13 December 2014. http://ria.ru/world/20140301/997697055.html

Security Council of the Russian Federation. 2000. Доктрина информационной безопасности Российской Федерации. (Information Security Doctrine of the Russian Federation.)

Security Council of the Russian Federation. 2009. Стратегия национальной безопасности Российской Федерации до 2020 года. (National Security Strategy to 2020.)

Security Council of the Russian Federation. 2013. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. (Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020.)

Security Council of the Russian Federation. 2014. Концепция стратегии кибербезопасности Российской Федерации. (Cyber Security Strategy of the Russian Federation – Concept.)

Seddon, M. 2014. “Documents Show How Russia’s Troll Army Hit America.” *Buzzfeed*, 2 June 2014. Accessed 20 December 2014. http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america

Security Service of Ukraine, SBU 2014. Служба безпеки України попереджає про “фейкові” електронні розсилки від імені державних органів. (Security Service of Ukraine warns of “fake” e-mails on behalf of public authorities.) 26 September 2014. Accessed 15 December 2014. http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=132039&cat_id=39574

Security Service of Ukraine, SBU 2015. СБУ: власники інтернет-спільноти “Антимайдан” знаходяться у Криму. (SBU: online community “Antimaidan” located in Crimea.) 13 March 2015. Accessed 15 March 2015. http://www.ssu.gov.ua/sbu/control/uk/publish/article;jsessionid=379798D64EB113AED76BBA26C5AE26A6.app1?art_id=138947&cat_id=39574

Shoigy, S. 2014. “Шойгу о российской технике в Крыму: ‘чушь и провокация’. (Shoigu on Russian military in Crimea: ‘nonsense and provocation’.)” *BBC Russkaya Sluzhba*, 5 March 2014. Accessed 2 December 2014. http://www.bbc.co.uk/russian/russia/2014/03/140305_crimea_troops_shoigu

Sindelar, D. “The Kremlin’s Troll Army.” *The Atlantic*, 12 August 2014. Accessed 20 December 2014. http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

Sivkova, A. 2014. “Флагман ВМФ Украины «Гетман Сагайдачный» перешел на сторону России. (Flagship the Ukrainian Navy, “Getman Sagaidachny“ defected to Russia.)” *Izvestiya*, 1 March 2014. Accessed 20. December 2014. http://izvestia.ru/news/566817

Symantec. 2014. Turla: Spying tool targets governments and diplomats. *Symantec*, 7 August 2014. Accessed 7 December 2014. http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

TASS. 2014a. “Число обращений граждан Украины в ФМС в Краснодарском крае увеличилось на 100%. (Number of requests for asylum by Ukrainians doubles in Krasnodar region.)” *TASS*, 26 March 2014. Accessed 20 December 2014. http://itar-tass.com/obschestvo/1075504

TASS. 2014b. “Граждане Украины просят временное убежище в Новгородской области. (Ukrainians request temporary asylum in Novgorod.)” *TASS*, 26 March 2014. Accessed 20 December 2014. http://itar-tass.com/spb-news/1076617

TASS. 2014c. “ФМС: за временным убежищем в РФ обратились более 245 тыс. граждан Украины. (FMS: Over 245k Ukrainians ask for asylum in Russia.)” *TASS*, 4 December 2014. Accessed 20 December 2014. http://itar-tass.com/obschestvo/1616949

TASS. 2014d. “Ukrainian frigate Hetman Sahaidachny carries NATO’s intelligence equipment — source.” *TASS*, 05 March 2014 Accessed 20 December 2014. http://tass.ru/en/world/722267

The Lithuanian Tribune. 2014. “Lithuania’s State Security Department warns citizens to beware of propaganda from Russia.” *The Lithuanian Tribune*, 5 September 2014. Accessed 17 December 2014. http://en.delfi.lt/lithuania/society/lithuanias-state-security-department-warns-citizens-to-beware-of-propaganda-from-russia.d?id=65761684

Tymchuk, D. 2014. “О предательстве. (On betrayal.)” *Gazeta.ua*, March 2014. Accessed 20 December 2014. http://gazeta.ua/ru/blog/42707/o-predatelstve

Unian. 2014. “Російські соціальні мережі втрачають популярність в Україні. (Russian Social Media loses popularity in the Ukraine.)” *Unian*, 30 July 2014. Accessed 20 December 2014. http://www.unian.ua/science/945549-rosiyski-sotsialni-mereji-vtrachayut-populyarnist-v-ukrajini.html

Umanec, V. 2014. “Як лоханувся телеканал ОРТ. (TV channel ORT failed.)” *Podglyad*, 2 March 2014. Accessed 17 December 2014. http://poglyad.te.ua/podii/yak-lohanuvsya-telekanal-ort/

Vorobyov, I. & Kiseljov V. 2013 “Russian Military Theory: Past and Present.” *Military Thought* 2013 (3).

YouTube. 2014. Database query: “Новости Новороссии”. *YouTube*. Accessed 13 December 2014.

Yuzhniy Kurier. 2014. “Все. Украинские солдаты в Крыму сдаются. (The End. Ukrainian soldiers in Crimea surrender.)” *Yuzhniy Kuri’er*, March 19, 2014. Accessed 20. December 2014. http://courier.crimea.ua/news/courier/vlast/1146781.html

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Technological Sovereignty: Missing the Point?

Tim Maurer
Open Technology Institute
New America
Washington, DC, USA
maurer@newamerica.org

Robert Morgus
Open Technology Institute
New America
Washington, DC, USA
morgus@newamerica.org

Isabel Skierka
Global Public Policy Institute
Berlin, Germany
iskierka@gppi.org

Mirko Hohmann
Global Public Policy Institute
Berlin, Germany
mhohmann@gppi.net

Abstract: Following reports of foreign government surveillance starting in June 2013, senior officials and public figures in Europe have promoted proposals to achieve "technological sovereignty". This paper provides a comprehensive mapping and impact assessment of these proposals, ranging from technical ones, such as new undersea cables, encryption, and localized data storage, to non-technical ones, such as domestic industry support, international codes of conduct, and data protection laws. The analysis focused on the technical proposals reveals that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance.

Keywords: *international affairs, foreign policy, cyber security, technological sovereignty, surveillance, encryption*

1. INTRODUCTION

In the months following the 2013 reports revealing surveillance by foreign governments, European government officials and public figures have promoted a variety of measures for gaining "technological sovereignty." The current German government's coalition agreement, for example, explicitly states that it will "take efforts to regain technological sovereignty."[1]

Technological sovereignty has been used as an umbrella term to suggest a spectrum of different technical and non-technical proposals, ranging from the construction of new undersea cables to stronger data protection rules. Many of them are not new but have developed greater political traction over the past year.

The main contribution of this paper is a comprehensive, systematic mapping and impact assessment of these technological sovereignty proposals.[2] Non-technical proposals such as a restructured Safe Harbor Agreement or a new European Union Data Protection Directive are also part of the debate and pose pros and cons of their own. However, that is outside the scope of this paper, which focuses on the technical measures and whether they will actually protect against foreign surveillance and gauge their impact on the open and free Internet. It builds upon existing literature,[3] but differs by distinguishing between types of proposals, and by considering whether they achieve their purported goal of protecting against foreign surveillance. This paper goes beyond analyses focused solely on data localization requirements[4] by providing a comprehensive overview of the proposals that have been advanced under the umbrella of technological sovereignty.

Research on the implications of these technological sovereignty proposals remains nascent. A growing body of literature examines the growth of "data localization" policies, meaning the "laws and guidelines which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, and companies."[5] Such proposals were the focus of attention in early 2014, because they were part of Brazil's debate over its Internet Bill of Rights, "Marco Civil da Internet." The term "technological sovereignty" remains vague. As it is used by European policymakers, it resembles terms like "data sovereignty," which has been defined as "a spectrum of approaches adopted by different states to control data generated in or passing through national [I]nternet." It is a subset of "cyber sovereignty," which is "the subjugation of the cyber domain to local jurisdiction."[6]

Our analysis builds on the scholarship and approach of Internet governance expert Laura DeNardis, who writes, "arrangements of technical architecture are also arrangements of power."[7] The Internet is a meta-network, composed of a constantly changing collection of individual networks and devices that communicate with each other through the Internet Protocol (IP). Through technical features, the physical and software architecture, or code, shapes human behavior on the Internet and beyond. Because the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. This architecture constitutes a powerful tool for actors to further their interests. Code "sets the terms upon which [actors] enter, or exist, in cyberspace."[8] According to Stanford law professor Barbara van Schewick, policymakers who traditionally used the law can now use Internet technologies to bring about desired political or economic effects.[9] Building upon this scholarship, we designed a framework for classifying the proposals based on what part of the Internet they impact.

Our research identified proposals from over a dozen countries in Europe, ranging from technical ones, like localized or nationalize routing schemes, to non-technical ones, like a European wide data protection authority. The majority of proposals are from Germany. They come from academia, the government, and the private sector and differ even within government as different ministries brought forth different proposals. Upon further examination of the technical proposals, our analysis shows that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance and ideas like the expansion of encryption tools that are more effective at securing data.

2. METHODOLOGY

We began this research by collecting proposals and statements[i] by European political decision-makers, as well as those of stakeholders from the private sector and academia, made after June 5, 2013, the day on which the first wave of articles about government surveillance was published.[ii] It is important to bear in mind that while these proposals were advanced in response to the surveillance affair, they address different dimensions of a complex problem, namely the protection of (1) government secrets; (2) individual citizens' privacy; and (3) industry secrets. An additional complexity is the fact that policymakers have been using the political attention to suggest new industrial policies aimed at supporting the European Information Technology (IT) sector through major public investments and IT sector-specific subsidies.

Upon completing the desk based collection phase of research, we proceeded in three steps to determine how each proposal affects the governing structures of the Internet, different types of data, and the Internet's underlying architecture.

Step 1: Dividing proposals into Two General Categories – Technical and Non-Technical

A first review of the proposals revealed that they could be clustered into two general groups: technical and non-technical proposals. We then grouped technical proposals based on the type of technological change proposed: new undersea cables, national e-mail, localized routing, encryption, and localized data storage. These proposals directly affect the technical architecture of the Internet. Non-technical proposals are those that affect the Internet in other ways – for example, calls for new laws or for more transparency, which could affect the technical architecture but indirectly so.

Technical proposals are based on the type of technological change proposed: new undersea cables, national e-mail, localized routing and storage, and encryption. New undersea cables, for example, refer to suggestions to directly connect Latin America and Europe, avoiding data transfer through the United States. Likewise, national e-mail was suggested in Germany as a means of avoiding contact with American servers whenever possible. Localized routing goes a step further than national e-mail, in the sense that it would encompass all data, not just e-mail data, and route it solely through local servers. However, localized does not necessarily mean that the data is concentrated in one country. For example, localized could encompass the

[i] These proposals and their sources are detailed in Figure 2.

[ii] For greater detail on this topic, see: Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

entirety of the European Union. Finally, there have been calls for improving encryption, making existing encryption more accessible to the general public, and extending it to mobile devices.

Non-technical proposals are sorted based on the changed mechanism: institution, law, norm, transparency, and business. The idea to establish a single EU Data Protection Agency exemplifies how actors consider institutions as a means of addressing a given challenge. A wide variety of laws have been proposed, and some implemented, ranging from changes to the US-EU Safe Harbor agreement[10] to domestic data protection laws. There are also several proposals aimed at increasing trust – not through regulation, but through the establishment of common norms, like a "no-spying" agreement between the US and European partners.[11] Another non-technological category is composed of proposals aimed at increasing transparency of how governments and businesses handle the data of citizens and customers. Proposals to advance the national production of hardware and software mainly originate in Germany, such as the "IT Security Made in Germany" brand or the production of an IT-Airbus in cooperation with France. Ideas like these fall into the business cluster, though there are technical components to the proposals. Generally, these non-technical proposals impact non-technical factors that shape the Internet, like laws, norms, markets, and institutions.

For the purposes of this paper, we focus on the proposals that have the highest likelihood of impacting the technical functionality of the Internet, which we call technical proposals.

Step 2: Determining Proposals' Political Traction

Some proposals have gained more political traction than others over the past year and a half. For our purposes, high political traction means that proposals have been widely discussed and have been implemented, or plans for implementation have been set. Other proposals have been discussed, but their implementation remains uncertain. These are classified as having medium political traction. Some proposals have been barely discussed or were discussed and discarded, and these are classified as having low political traction.[iii]

Step 3: Integrating Different Types of Data: Data in Motion, Data at Rest, and Metadata

To elevate the level of technical acumen informing this debate, it is important to note that several types of data exist: data in motion, data at rest, and metadata. Governance proposals depend on what type of data is to be governed.

The data we access on the Internet is stored on servers. When this data is inactive – meaning, it is not being changed or in motion – it is classified as data at rest. Data at rest can be the text, music, or video files we store in the cloud, or the data that is the content of a webpage stored on a company server.

Data in motion is data that traverses the physical infrastructure of the Internet. Because the Internet is a global network of computing devices, from laptops and PCs to smart phones, data must flow from the host device or server to the device trying to access it. The easiest way to explain this phenomenon is to picture an e-mail sent from one user to another. The sender generates the data that then travels over the cables and wires that make up the physical

[iii] We explain the degree of political traction of the technical proposals in the Impact Analysis, section 3.

infrastructure of the Internet, until it reaches the intended recipient. The same process happens when a user tries, for example, to access content through a webpage or download videos from a server. The route taken by the data depends on a number of factors, ranging from physical constraints like bandwidth to contractual considerations like peering agreements. Nonetheless, data is generally routed through what technologists refer to as the "cheapest" route. This ensures that the data reaches its recipient quickly and keeps Internet speeds high for everyone.

Metadata, simply put, is the data about data. Two types exist. Structural metadata "indicates how compound objects are put together."[12] This type of metadata is mostly used to present complex items. Structural metadata takes two separate streams of data, identifies them, and then ensures that they are properly synchronized for presentation. In other words, structural metadata ensures that the visual stream of the latest movie you are watching is synchronized with the audio stream. The second type of metadata is descriptive metadata, which "describes a resource for purposes such as discovery and identification."[13] This is the conceptualization of metadata. Descriptive metadata allows users to query databases and to identify data based on relevant criteria. It should be noted that even encryption does not necessarily protect metadata from surveillance. Figure 2 visualizes how the proposals are clustered.

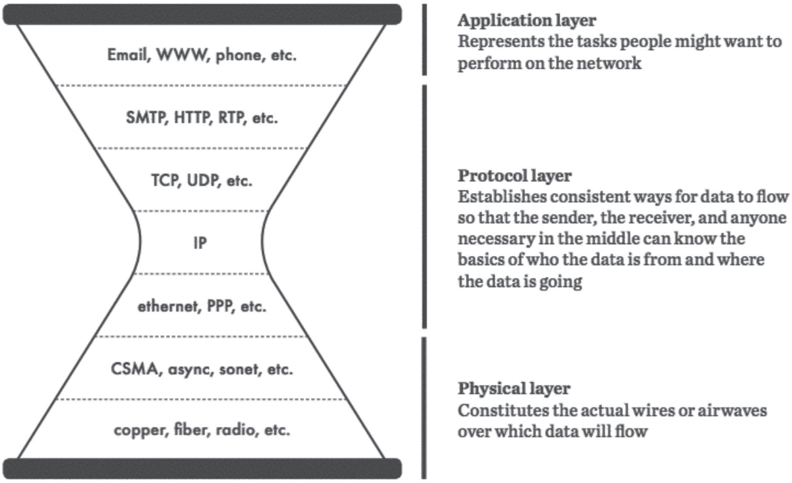
Step 4: Zooming in on Data in Motion: the Hourglass Model

Several models exist to illustrate the intricacies of the technical architecture that underlies the Internet. Internet expert and Harvard law professor Jonathan Zittrain built upon those and the work of many other scholars by combining the technical and social components of the Internet with his interpretation of the Hourglass Model, which highlights the centrality of the IP for the Internet's coherence and interoperability.

At the bottom is the physical layer, or "the actual wires or airwaves over which data will flow."[14] Undersea and fiber-optic cables are physical examples of the physical layer, as are the servers that receive them and the satellites that transmit a limited amount of Internet traffic. Next is the protocol layer, which "establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of whom the data is from and where the data is going."[15] This layer includes the limited IP, as well as the HTTP and the Simple Transportation Management Protocols (STMP). The IP layer is the narrowest layer in the hourglass model, signifying that it is, for the time being, the least elastic feature of the Internet, but also the layer on which the rest rely for communication. While we can build new cables and add more end-user devices, we are constrained by a finite number of IP addresses. Moving up the Hourglass, we find the application layer, "representing the tasks people might want to perform on the network."[16] E-mail clients and websites, for example, make up this layer. Resting atop the Hourglass are Zittrain's final two layers: the content layer, which is the actual information exchanged through the other layers, and the social layer, "where new behaviors and interactions among people are enabled by the technologies underneath."[17] These layers and the implications they carry apply directly to the proposals that we classify as technical proposals.

The architecture constraint in real space is the constraint of code in cyberspace. As the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. That’s why the technical proposals are a specific focus of this paper.

FIGURE 1: THE HOURGLASS MODEL



Application layer
Represents the tasks people might want to perform on the network

Protocol layer
Establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of who the data is from and where the data is going

Physical layer
Constitutes the actual wires or airwaves over which data will flow

Source: Zittrain, Jonathan (2008) *The Future of the Internet and How to Stop It*. Yale University Press. p. 67-68.

FIGURE 2: TECHNICAL PROPOSALS

Type of Proposal	Summary	Proposing Actors	Country or Region	Time Range	Data Type	Layer	Political Traction
New Undersea cables	Lay a new fiber-optic submarine cable between Latin America and Europe; lay a new fiber-optic cable between Finland and Germany, circumventing Sweden[18, 19]	Public: Herman Van Rompuy[iv] Krista Kiuru[v]	EU, Finland	12/11/2013 - 2/24/2014	Motion	Physical	High
Localized routing	Data streams should flow within a geographically restricted zone; inter-Schengen data traffic should be routed within the Schengen zone[20, 21, 22, 23, 24, 25]	Public: German government Private: Deutsche Telekom, Atos	France, Germany	10/12/2013 - 7/27/2014	Motion + Meta	Protocol (Content, Applica-tion, Physical)	Medium

[iv] President of the European Council.

[v] Finnish Minister of Education, Science and Communication.

National e-mail	Route all e-mails within Germany on German servers and cables[26]	Private: Deutsche Telekom	Germany	8/1/2013	Motion + Meta	Application	High
Localized data storage	Create a European or a Schengen cloud; create a European or Schengen zone for data[27, 28, 29, 30]	Public: French, German governments Private: Green,[vi] Deltalis,[vii] Quantique,[viii] EuroCloud[ix]	France, Germany, Poland, Switzerland	6/27/2013 - 5/14/2014	Rest + Meta	Data at rest	High - Medium
Expansion of encryption tools	End-to-end encryption of communication data; encryption of end devices;[31, 32, 33] End-to-end mobile voice encryption;[34, 35] Secure SIM data for corporate customers[36]	Public: European Parliament, Academia: Stefan Katzenbeisser,[x] Mark Manulis[xi]	Germany, UK	11/23/2013 - 2/24/2014	Motion + Rest	Protocol, Content, Application, Physical, and Data at rest	Medium

3. IMPACT ANALYSIS

This impact analysis examines whether the proposals actually achieve their purported goals of making data more secure in response to the surveillance debate, and then assesses the proposals' broader implications for the Internet, using the 2011 OECD Principles for Internet Policy-Making.[37]

The OECD principles provide concise guidance for policymakers crafting Internet policy, and they were designed to "help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives."[38] Given that the OECD member countries, as well as multiple other stakeholders, agreed upon these principles, they offer a useful anchor for transatlantic cooperation. We identified eight out of the 14 principles that are relevant to technological sovereignty and grouped them into four categories that constitute the foundation for our analysis of the proposals:[xii]

Human Rights:

OECD #1:	Promote and protect the global free flow of information.
OECD #9:	Strengthen consistency and effectiveness in privacy protection at a global level.

[vi] Switzerland.

[vii] Switzerland.

[viii] Switzerland.

[ix] Poland.

[x] Technische Universität Darmstadt, Germany.

[xi] University of Surrey, United Kingdom.

[xii] For a full list and explanation of the principles, see Annex 3 of Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

Governance – Open Internet:

OECD #2: Promote the open, distributed, and interconnected nature of the Internet.
OECD #8: Ensure transparency, fair process, and accountability.

Economic:

OECD #4: Promote and enable the cross-border delivery of services.
OECD #11: Promote creativity and innovation.

Security:

OECD #13: Encourage cooperation to promote Internet security.
OECD #14: Give appropriate priority to enforcement efforts.

New Undersea Cables

Public sector officials have suggested laying new undersea cables in order to circumvent foreign surveillance. Laying new undersea cables alters the physical layer of the Internet's architecture over which data will flow and does not harm the free flow of information *per se*. However, new undersea cables are not an effective strategy to protect against foreign surveillance because foreign law enforcement and intelligence agencies are adept at tapping undersea cables.[39] Thus, proposals for new undersea cables as a means to avoid foreign surveillance creates a false sense of security for users. While new and more undersea cables can positively contribute to an interconnected and distributed Internet, they do not make data more secure.

Localized Routing

Parts of both the public and private sectors have suggested the implementation of localized routing. These schemes require the alteration of transmission protocols that dictate how data flows over the physical architecture of the Internet. However, despite physically altering the location of data flows, localized routing does not effectively protect data from foreign surveillance. For this reason, legally mandated localized routing schemes have lost nearly all their political traction in Europe. It would also make law enforcement easier, as data would be subject to national data protection laws, which usually contain law enforcement exemptions.[40] Therefore, the localization of routing is unlikely to actually secure communications and risks providing a false sense of security to Internet users.

Mandatory localized routing requirements could also have dire consequences for the Internet as a whole. It would require changes to the routing protocols and IP address allocation system, contra to one of the Internet's fundamental principles that data flows via the cheapest or most efficient route. Whether or not a localized routing scheme negatively affects the free flow of information depends on the rule of law in the location in question. This enhances domestic private and state actors' control over information and data flows, and several authoritarian regimes have sought to implement localized routing to increase their own control over data flowing across the Internet infrastructure geographically located within their country.[41] It should be noted that there has also been a debate about "Network Security Agreements" between the U.S. government and foreign telecommunications providers, such as Deutsche Telekom, to localize routing of national data traffic.[42]

National E-Mail

National e-mail schemes, like E-Mail Made in Germany, were proposed and implemented by both Deutsche Telekom and United Internet, who are serving more than two thirds of e-mail users in Germany.[43] However, because the proposed service does not use a higher than normal security standard to this date it will not protect against surveillance any better than existing services of which many have used the Simple Mail Transfer Protocol Secure (SMTPS) with Transport Layer Security (TLS) for years already.[44] Moreover, the E-Mail Made in Germany initiative has been criticized for using a proprietary standard for secure data transmission (the "Inter Mail Provider Trust") instead of the openly available standard DANE (DNS-Based Authentication of Named Entities), which other smaller competitors have been using and is more easily auditable.[45] Finally, if data is stored unencrypted on the e-mail provider's servers, it can still be intercepted regardless of the encryption used for the data in transit.

National e-mail could in fact make law enforcement easier, since data is stored within national borders and subject to national data protection laws, which usually contain enforcement exceptions.[46] The proposed service highlights the risk of promoting proposals that give users a false sense of security by claiming enhanced security features without actually significantly enhancing security.

Localization of Stored Data

Both public and private sector officials have proposed mandating localized data storage. Proposals to territorially localize data storage seek to store all data generated by Europeans on servers located in Europe. This action will not effectively protect data from surveillance and actually concentrates the data in a number of defined physical locations, potentially narrowing the search for intelligence and law enforcement agencies seeking specific data.

Adding to that, legal barriers for foreign intelligence agencies are often less strict when collecting data internationally. Although data stored in Europe is subject to EU data protection laws, this does not mean that the parties that own the data are exclusively subject to those same laws. Therefore, the security of data from foreign intelligence agencies depends not on where it is stored, but on comprehensive security practices, modern technology, and qualified security personnel.[47] Similar to other localization proposals, it risks providing a false sense of security to users.

Localized data storage would also harm the open and distributed nature of Internet, by forcing the "nodes" to be located in specific geographic areas, where their operations might be suboptimal from a global perspective.

Requiring localized data storage would impede cross-border delivery of services and raise costs and barriers to entry, particularly for smaller companies, which in turn risks hampering innovation.[48]

For these reasons, no steps have been taken to date to legally mandate localized data storage. Instead, policymakers have turned to the promotion of voluntary data security standards. For example, the European Commission issued the Common Service Level Agreements for Cloud Computing[49] and the European Cloud Partnership, which suggest common, non-binding security and encryption standards for European cloud providers storing data on European soil.[50]

Expansion of Encryption Tools

Suggestions to expand encryption tools have come from the public sector and academia. While encryption may not protect individuals against sophisticated, targeted surveillance by intelligence agencies, the widespread use of encryption would significantly raise the cost of surveillance generally. The more individuals encrypt their communications, the more difficult and costly it will to decrypt those communications. Encryption can be applied to all layers of the Internet – to the physical layer (cable or radio communications), the protocol layer (i.e, Hypertext Transfer Protocol [HTTP] or Transmission Control Protocol [TCP]), and the application layer (e-mail, www, mobile). Thus, encryption can protect both data in motion through end-to-end encryption of communications, as well as data at rest through encryption of devices or servers at the end nodes.

Calls for stronger encryption have received growing political traction around the world. Several experts have called for the development of more easily accessible encryption tools,[51] and the European Parliament has called on the European Commission to "strengthen the protection of confidentiality of communication … by way of requiring state-of-the-art end-to-end encryption of communications."[52] Major technology companies like Apple and Google have also begun offering encryption by default,[53] and the Internet Engineering Task Force (IETF) has resumed work on building encryption by default into HTTP 2.0 after the initial surveillance reports, a project it had previously decided against in March 2012.[54]

The different forms of encryption tools proposed in Europe attempt to deliver better privacy through end-to-end encryption of mobile voice communication. The use of crypto phones can be an effective tool for protecting government and business secrets and individuals' private data. Various proposals also advocate for better end-to-end encryption of e-mail, instant messaging, cloud storage, and radio. Existing tools are often difficult and cumbersome to use, so engineers at the IETF and major US software companies are working on making encryption more easily accessible to the wider public.[55] It is possible for data encrypted from end-to-end to be accessed by intelligence or law enforcement agencies, but only through measures targeted at specific users and with much greater difficulty. While encryption enhances the protection of both data in motion and at rest, it does not necessarily protect metadata.

Different forms of encryption can be applied to various layers of the Internet while preserving its decentralized structure and strengthening the capacity of actors within the existing frameworks. Therefore, the use of encryption tools has no negative impact on the free flow of information. As long as encryption is promoted globally and encryption tools can be imported and exported without national restrictions, proposals to enhance encryption efforts can promote innovative, easier-to-use technologies. The use of encryption technologies strengthens overall Internet security, as well as individual and collective efforts for self-protection. However, encryption proposals are not without drawbacks.

First, encryption tools are generally regarded as difficult and cumbersome to use and adoption of strong encryption, though available, has been slow.[56] Second, law enforcement and counterterrorism agencies point to a tension between data privacy and national security and law enforcement.[57] Law enforcement in the United States, in particular, has argued that the expansion of encryption lends itself to the "going dark" problem and severely hinders law enforcement investigations.[58] Some have consequently advocated for a "golden key" to encrypted devices and communications, which should be provided to or stored with a third party, such as a trusted authority under the state's jurisdiction. However, such backdoors and keys stored elsewhere constitute a risk for Internet security, since they could be exploited by criminals.[59] This topic and how to approach physical and virtual security has been the subject of an emerging and important debate in the United States and the United Kingdom.[60]

4. CONCLUSION

Calls for technological sovereignty have not been limited to Europe. In Brazil, data localization proposals were hotly debated. In China, government offices are prohibited from using the Windows 8 operating system, and Cisco and IBM are under scrutiny.[61] The Australian government has banned China's Huawei from participating in building its National Broadband Network. And the United States has not been immune from this trend, as portrayed by Congress's creation of a cyber espionage review process in 2013 to limit government procurement of Chinese IT equipment.[62] Moreover, under "Network Security Agreements," the U.S. government legally obliges foreign communication infrastructure providers such as Deutsche Telekom to route their traffic exclusively within U.S. borders.[63]

This in-depth analysis of the European technological sovereignty proposals reveals several trends. First, it is unlikely that most technical proposals proposed to date will effectively protect data against surveillance from foreign government intelligence agencies. Only a limited number of proposals might achieve that – namely encryption – and they have not been at the center of attention in the European debate. Second, some proposals could in fact have a negative effect on the open and free Internet, or at least lead to an inefficient allocation of limited resources. Moreover, the specific impact often depends on how the proposals are implemented and remains uncertain without further research. Third, the proposals tend to be narrowly focused on the transatlantic dimension and generally neglect the larger challenge and the new technological reality. Finally, especially in the case of the expansion of encryption tools, tensions between privacy advocates, private companies, and law enforcement and national security officials emerge.

The impact of proposals often depends on the details of their implementation, which remain unknown to date. On the surface, a proposal might appear to have a positive impact but a closer look casts doubt on their effectiveness. For example, increasing funding for small businesses and establishing an "IT Security Made in Germany" brand will only increase data security if those companies produce, and are capable of producing, products and services with higher security standards than those of foreign companies. So far, the implementation of these proposals does not suggest that they offer significantly more secure services, which in some cases instead provides a false sense of security.

At first blush, restricting data from flowing through the physical infrastructure of other countries might seem like an effective measure for protecting against government surveillance. However, this is a false hope. Moreover, the laws in some countries lower the legal barrier for intelligence agencies to collect and analyze data if the data is collected outside of the intelligence agency's home country.[64] This reality means that measures forcing data to remain within a country's borders might lower the legal threshold for foreign intelligence agencies to conduct surveillance in the first place. Proposals focused on simply physically avoiding certain countries misunderstand current technological and legal realities and risk wasting important resources that could be used to effectively make data more secure.

Data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted. A critical fact often ignored in the debate thus far is that the governments exposed by media reports since June 5, 2013 are unlikely to be the only countries with such technical surveillance capabilities. The issue is global, not Transatlantic, in nature and the challenge is the result of a new technological reality. It therefore requires a broader debate and approach. The proposals most likely to protect against any foreign surveillance focus on encryption tools. These deserve greater attention and scrutiny if the goal is to secure data more effectively.

ACKNOWLEDGMENT

The authors would like to thank the members of the Steering Committee for the project Transatlantic Dialogues on Security and Freedom in the Digital Age (go to www.digitaldebates.org for more) as well as the participants of the workshops hosted in Washington, DC, and Berlin for their valuable input and feedback. All views, errors or omissions are solely the authors' responsibility.

REFERENCES

[1] German Government. 2013. "Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode." <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=2820F3157BAD69B7313E63020CF9944C.s4t2?__blob=publicationFile&v=2>.

[2] A comprehensive list of proposals can be found in Annex II.

[3] Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders." *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>; Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet." *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[4] Chander, Anupam and Uyen P. Le. 2014; Hill, Jonah Force. 2014.

[5] Chander, Anupam and Uyen P. Le. 2014. “Breaking the Web: Data Localization vs. the Global Internet.” *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>.

[6] Polatin-Reuben, Dana and Joss Wright. 2014. “An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet.” *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[7] DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press, p. 9.

[8] Lessig, Lawrence. 1998. “The Laws of Cyberspace.” *Presented at the Taiwan Net ’98 Conference*. p. 4.

[9] van Schewick, Barbara. 2010. *Internet Architecture and Innovation*. Cambridge: MIT Press.

[10] The Safe Harbor agreement is the process developed by the US Department of Commerce that allows US companies to more easily comply with EU Directive 95/46/EC, the initial EU Data Protection Directive from 1998. When the directive went into force in 1998, “it became clear that it actively threatened data flows between the two largest trading partners on earth.” Thus, the Safe Harbor agreement, which is unique to the US and EU, is “voluntary self-certification system for transmitting data from the EU to the United States.” For more on the Safe Harbor, see: Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 12. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[11] O’Donnell, John and Baker, Luke. 2013. “Germany, France demand ‘no-spy’ agreement with U.S.” *Reuters*. Oct. 24. <http://www.reuters.com/article/2013/10/25/us-eu-summit-idUSBRE99N0BJ20131025>.

[12] National Information Standards Organization. 2004. *Understanding Metadata*. NISO Press, p. 1-2. <http://marciazeng.slis.kent.edu/metadatabasics/types.htm>.

[13] Ibid.

[14] Zittrain, Jonathan L. 2008. *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press, Chapter 4, p. 67-100.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] European Council: The President. 2014. “Press Statement by the President of the European Council, Herman Van Rompuy, following the 7th EU-Brazil Summit.” *The European Council*. <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf>.

[19] Ronnholm, Antton. 2014. “Minister Kiuru on submarine cable decision: Finland to be a safe harbor for data.” *Finnish Ministry of Transport and Communications*. Apr. 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>.

[20] Berke, Jürgen. 2013. “Telekom will innerdeutschen Internetverkehr ubers Ausland stoppen.” *Wirtschafts Woche*. Oct. 12. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html>.

[21] Schäfer, Louisa. 2013. “Deutsche Telekom: ‘Internet data made in Germany should stay in Germany.’ Interview with Philipp Blank.” *Deutsche Welle*. Oct. 18. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>.

[22] Gaugele, Von Jochen, Kade, Claudia, Malzahn, Claus Christian and Vitzthum, Thomas. 2014. “Dobrindt will mit ‘Netzallianz’ an die Weltspitze.” *Die Welt*. Jan. 12. <http://www.welt.de/politik/deutschland/article123774038/Dobrindt-will-mit-Netzallianz-an-die-Weltspitze.html>.

[23] Thombansen, Hannah. 2014. “Video-Podcast der Bundeskanzlerin #2/2014.” *Bundesregierung*. Feb. 15. <http://www.bundesregierung.de/Content/DE/Podcast/2014/2014-02-15-Video-Podcast/links/download-PDF.pdf;jsessionid=0BC9A500E8D948E37C285341160692B2.s4t1?__blob=publicationFile&v=3>.

[24] Breton, Thierry. 2013. “Atos CEO calls for ‘Schengen for data.” *Thierry Breton’s blog*. Sept. 2. <http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>.

[25] von Altenbockum, Jasper und Lohse, Eckart. 2014. “Verfassungsschutz-Präsident ‘Wir werden unsere Abwehr verstärken.’” *Frankfurter Allgemeine Zeitung*. July 28. <http://www.faz.net/aktuell/politik/inland/interview-mit-hans-georg-maassen-abwehr-verstaerken-13067331.html>.

[26] Deutsche Telekom. 2013. “Deutsche Telekom, WEB.DE and GMX launch ‘E-mail made in Germany’ initiative.” *Deutsche Telekom Media*. Aug. 9. <http://www.telekom.com/media/company/192834>.

[27] Iwankiewicz, Maciej W. 2013. “The Polish Approach to EU Cloud Computing Strategy.” *EuroCloud*. July 5. <http://www.eurocloud.org/the-polish-approach-to-the-eu-cloud-computing-strategy/>.

[28] Deutscher Bundestag. 2013. “Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.” *German Bundestag*. Nov. 15. <http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf>.

[29] Juskailian, Russ. 2014. “For Swiss Data Industry, NSA Leaks Are Good as Gold: here’s how the Swiss promise to keep your data safe.” *Technology Review*. Mar. 18. <http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/>.

[30] Le Maire, Bruno. 2014. “Bruno Le Maire: Pour un Cloud europeen.” *Slate*. May 14. <http://www.slate.fr/tribune/87057/bruno-le-maire-cloud-europeen>.

[31] European Parliament. 2014. “Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs.” Feb. 21. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[32] Ward, Mark. 2014. “Can Europe go its own way on data privacy?” *BBC Technology*. Feb. 17. <http://www.bbc.com/news/technology-26228176>.

[33] Schutz, Colin. 2014. “Tech Companies Are Trying to Make NSA-Proof Encrypted Phones and Apps.” *Smithsonian Magazine*. Feb. 24. <http://www.smithsonianmag.com/smart-news/tech-companies-are-responding-nsa-revelations-encrypted-phones-and-apps-180949874/?no-ist>.

[34] Sawall, Achim. 2013. “Simko 3 zugelassen.” *Golem.de*. Sep. 9. <http://www.golem.de/news/simko-3-zugelassen-hintertueren-lassen-sich-bei-smartphones-nicht-ausschliessen-1309-101467.html>.

[35] Deutsche Telekom. 2013. “Data Privacy and Data Security: Report 2013.” *Deutsche Telekom AG*. <http://www.telekom.com/dataprotection>.

[36] Gandhe, Shreyas. 2014. “Vodafone Germany starts rolling out SIM card based encryption.” *Neowin.net*. Mar. 12. <http://www.neowin.net/news/vodafone-germany-starts-rolling-out-sim-card-based-encryption>.

[37] OECD. 2011. “Communiqué on Principles for Internet Policy-Making.” *OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth*. June 29. p. 3. <http://www.oecd.org/internet/innovation/48289796.pdf>.

[38] Ibid.

[39] Khazan, O. 2013. “The Creepy, Long-Standing Practice of Undersea Cable Tapping.” *The Atlantic*. Jul. 16. <http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>.

[40] Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[41] See, for example: Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. “Internet Censorship in Iran: A First Look.” *Censorship Project*. Aug. <https://jhalderm.com/pub/papers/iran-foci13.pdf>; and Roberts, Hal, David Larochelle, Rob Faris, and John Palfrey. 2011. “Mapping Local Internet Control.” *Berkman Center for Internet & Society at Harvard University*. May 13. <http://cyber.law.harvard.edu/netmaps/mlic_20110513.pdf>.

[42] Public Intelligence. 2013. “U.S. Government Foreign Telecommunications Providers Network Security Agreements”. <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[43] Deutsche Telekom. 2014. <http://www.telekom.com/medien/produkte-fuer-privatkunden/220370>.

[44] Dierks, T. and E. Rescorla. 2008. “The Transport Layer Security (TLS) Protocol Version 1.2.” *Internet Engineering Task Force Network Working Group*. <http://tools.ietf.org/html/rfc5246>.

[45] Emert, M. 2014. “RIPE diskutiert bedenkliche Entwicklungen: Das Google-Net und EmiG”. 19 May. < http://www.heise.de/netze/meldung/RIPE-diskutiert-bedenkliche-Entwicklungen-Das-Google-Net-und-EmiG-2192176.html>.

[46] Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[47] Bob Butler, Irving Lachow, Jonah Force Hill. 2014. “Cloud computing under siege.” *Few.com*. Sept. 12. <http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx>.

[48] Plaum, Alexander. 2014. “The impact of forced data localisation on fundamental rights.” *Access Now*. April 4.. <https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights>.

49] European Commission. 2014. “Cloud Service Level Agreement Standardisation Guidelines”. <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.

[50] European Cloud Partnership Steering Board. 2014. “Establishing a Trusted European Cloud.” <http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf>.

[51] Waidner, Michael. 2014. "Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014." June 26. <https://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf>.

[52] European Parliament. 2014. "Motion for a European Parliament Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." *European Parliament*. Feb. 21. Paragraph 95. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[53] Vance Jr., Cyrus R. 2014. "Apple and Google threaten public safety with default smartphone encryption." *The Washington Post*. Sept. 26. <http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html>.

[54] Jackson Higgins, Kelly. 2013. "NSA Leaks Bolster IETF Work On Internet Security." *DarkReading*. Nov. 14. <http://www.darkreading.com/risk/nsa-leaks-bolster-ietf-work-on-internet-security/d/d-id/1140891>.

[55] Protalinski, Emil. 2014. "Gmail now always uses an HTTPS connection and encrypts all messages moving internally on Google's servers." *The Next Web*. Mar. 20. <http://thenextweb.com/google/2014/03/20/gmail-now-uses-encrypted-https-connection-check-send-email/>; Armasu, Lucian. 2014. "Huge: Cloudflare's Free SSL Service Brings Encrypted-By-Default Web Closer Than Ever." *Tom`s Hardware*. Sept. 29. <http://www.tomshardware.com/news/cloudflare-security-encryption-ssl-https,27780.html>; Perey, Juan Carlos. 2014. "Microsoft makes email encryption for Office 365 easier." *Tech Central.ie*. Oct. 6. <http://www.techcentral.ie/microsoft-makes-email-encryption-office-365-easier/#ixzz3Ix0eOXHl>; O'Neill, Patrick Howell. 2014. "Tor executive director hints at Firefox integration." *The Daily Dot*. Sept. 29. <http://www.dailydot.com/politics/tor-mozilla-firefox/>; Meyer, David. 2014. "Pretty Easy Privacy project aims to make encryption easier for regular people to use." *Gigaom*. Oct. 6. <https://gigaom.com/2014/10/06/pretty-easy-privacy-project-aims-to-make-encryption-easier-for-regular-people-to-use/>.

[56] For a broader discussion of the usability of encryption, see: Lee, Timothy B. 2013. "NSA-proof encryption exists. Why doesn't anyone use it?" Washington Post. June 14. <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/>.

[57] For more on this debate in the UK, see: Price, Rob. 2015. "David Cameron Wants to Ban Encryption." *Business Insider*. Jan. 12. <http://www.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1>.

[58] FBI Director James Comey has been particularly outspoken on this issue. For more, see: Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>.

[59] Schneier, Bruce. 2014. "Stop the hysteria over Apple encryption." *CNN*. Oct. 31. <http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/>.

[60] The Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *The Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>; Street, Jon. 2014. "Eric Holder: Apple, Google Not Giving Law Enforcement Access to Encrypted Data Is 'Worrisome.'" *The Blaze*. Oct. 1. <http://www.theblaze.com/stories/2014/10/01/ eric-holder-apple-google-not-giving-law-enforcement-access-to-encrypted-data-is-worrisome/>; Hosko, Ronald T. 2014. "Apple and Google's new encryption rules will make law enforcement's job much harder." *The Washington Post*. Sept. 23. <http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>.

[61] Tiezzi, Shannon. 2014. "In Cyber Dispute With US, China Targets IBM, Cisco." *The Diplomat*. May 28. <http://thediplomat.com/2014/05/in-cyber-dispute-with-us-china-targets-ibm-cisco/>.

[62] Rogers, Mike and Dutch Ruppersberger. 2012. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Permanent Select Committee on Intelligence. Oct. 8. <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>.

[63] Public Intelligence. 2013. "U.S. Government Foreign Telecommunications Providers Network Security Agreements". <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[64] Willis, Aidan. 2010. "Guidebook: Understanding Intelligence Oversight." *Geneva Centre for the Democratic Control of Armed Forces (DCAF)*. <http://www.dcaf.ch/Publications/Guidebook-Understanding-Intelligence-Oversight>.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe

Sergei Boeke LL.M.
Leiden University Centre for Terrorism
and Counterterrorism
The Hague, The Netherlands

Matthijs A. Veenendaal
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Caitríona H. Heinl
Centre of Excellence for
National Security
S. Rajaratnam School of
International Studies
Singapore

Abstract: While many states are developing national cyber security strategies, the exact role and responsibilities of the armed forces in cyberspace often remain unclear. Although attention has been devoted to acquiring specific technical capacities and expertise to act in cyberspace, decision-making processes, doctrines for deployment, and procedures generally lack systematic analysis. The first part of this article therefore focuses on whether militaries in their own national context contribute to defensive cyber security tasks. Common national challenges are identified, as are approaches that potentially improve cyber security through better civil-military cooperation. The article then examines the organisational structures in place across Asia and Europe to enable better international military cooperation for cyber related incidents. It outlines how international cooperation might assist a better exchange of information to increase cyber defence effectiveness, specifically between Asia and Europe.

Keywords: *cyber defence, civil-military relations, international military cooperation, Europe, Asia*

1. INTRODUCTION

As cyber security is increasingly conflated with national security, there is debate on whether cyberspace is being militarised.[1] Armed forces across the globe are investing in their capacity to defend their networks and systems, and increasingly, preparing to conduct military operations in cyberspace. While alarmists in academia and politics warn of the threat of ‘a digital Pearl Harbor’ or a ‘cybergeddon’, potentially paralysing a connected society,[2] the question of how armed forces can or should contribute to enhancing and protecting national and international cyber security, outside of an armed conflict, has not been fully answered yet and has thus far received limited academic attention.

This article therefore aims to investigate the challenges faced by different European and Asian nations in defining the role of the armed forces regarding cyber security and how these are formulated in official national documents. The focus lies exclusively on the militaries’ defensive tasks, excluding possible ‘offensive operations’. This article builds on the results of a workshop organized by the S. Rajaratnam School of International Studies (RSIS), Singapore and Leiden University Centre for Terrorism and Counterterrorism (CTC), which was held in Singapore in November 2014 and made possible by the ministry of defence of the Netherlands.

The article is divided into two sections. The first section examines the military’s role in national cyber security while the second section considers the structures in place across Asia and Europe to enable better international military cooperation for cyber related incidents between the two regions.

2. THE MILITARY’S ROLE IN NATIONAL CYBER SECURITY

This section focuses on the challenges involved in defining and clarifying the responsibilities of the armed forces regarding the protection of national security and how these relate to civilian authorities. Common national challenges are identified, as are approaches that potentially improve cyber security through better civil-military cooperation.

The growing dependence of critical infrastructure on digital technology has been generally recognized and, consequently, the protection of national critical infrastructure is a central tenet in most cyber security strategies and policies. The way in which cyberspace is structured and governed means that the digital domain presents several challenges when it comes to protecting national security. In cyberspace, the classical distinctions between military and civil, public and private and national and international actors are less clear-cut. For instance, as critical infrastructure is predominantly run by the private sector in most countries across Europe and Asia, although not all, some form of public-private partnership for crisis management and

[1] See for instance Ronald J. Deibert, ‘*Black Code: censorship, Surveillance and the increasing Militarization of Cyber space*’, Journal of International Studies, December 2003 vol. 32 no. 3 501-530 and Myriam Dunn Cavelty (2012), ‘*The Militarisation of cyberspace, Why less may be better*’, Proceedings of the 4th International Conference on Cyber Conflict (Tallinn, 2012).

[2] See for instance Richard Clarke and Robert Knake, ‘*Cyber War: The Next Threat to National Security and What to Do About It*’, (New York, 2010) and Leon Panetta, *Defending the Nation from Cyber Attack*”, speech delivered at Business Executives for National Security, New York, October 11, 2012. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728 [accessed March 2015].

incident response is necessary.[3] While many approaches are possible, ranging from stimulating self-regulation to interventionist government policies, complex issues remain related to the way in which governments address their responsibility for the protection of critical infrastructure.[4]

In both Asia and Europe, different ministries are responsible for coordinating cyber security issues and critical infrastructure protection. These ministries range from the ministry of justice (as is the case in the Netherlands and Indonesia), the ministry of the interior (Estonia and Germany), the ministry of technology or information technology (India, Malaysia and Thailand), to the ministry of defence (Denmark). The varied way of conferring responsibility has its origins in different factors, such as historical context, domestic considerations, and wider geostrategic concerns. The consequences, however, are significant as the legal mandate can vary per sector, with ministries of the interior or home affairs predominantly concerned with public order, ministries of justice with law enforcement and ministries of defence with national security. From this perspective it would be logical for a country which considers cyber crime the most serious threat to mandate the justice ministry with the coordination of cyber security, while one fearful of state sponsored espionage or cyber conflicts should be more inclined to give a lead role to defence organisations. While more research is certainly warranted in this area, it appears that, although national policies and strategies certainly reflect perceived cyber threats, the institutional embedding of roles and responsibilities in the cyber domain often follows a different logic and is more a result of specific political and organizational traditions and processes.

National perspectives on whether to focus on the opportunities or threats of cyberspace also differ within both Asia and Europe. In Asia, for instance, countries such as Laos and Cambodia have a low ratio of Internet connectivity, and, given their less cyber dependent critical infrastructure, their cyber security policies are developed more from the perspective of the opportunities these offer for economic growth. India also has a cyber policy that focuses strongly on the economic policies.[5] Some countries like Spain and Thailand seem most concerned about cyber crime and malicious cyber activities from non-state actors. Although cyber crime is described by many countries as the major threat in Asia and Europe, simmering interstate tensions and a host of cyber incidents that have been kept from public view imply that the securitisation[6] of cyberspace is perhaps more acute but less acknowledged in Asia. South Korea, for example, is formally still at war with North Korea, and, together with Japan, the country has been the target of cyber attacks, indicating North Korean involvement.[7] Central to the Asian geopolitical context is the position of China and the perceived United States pivot to the Asian Pacific, and several countries in Southeast Asia are involved in long-standing territorial or maritime disputes with China. Some countries estimate that the most serious threat emanates from state-sponsored cyber activities. Irrespective of official threat analyses, the distinction between cyber

[3] Myriam Dunn-Cavelty & Manuel Suter, 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, Volume 2, Issue 4, December 2009, pages 179–187.

[4] Ibid.

[5] National Cyber Security Policy of India (2013). Retrieved in March 2015 from: http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

[6] Securitization means that "[an issue] is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure." Security ''frames the issue either as a special kind of politics or as above politics.'' (in *Security: A New Framework for Analysis*, Barry Buzan et al. 1998, p. 23).

[7] See for instance the Choe Sang-Hun, '*Computer networks in South Korea are paralyzed by cyber attacks*', The New York Times, 20 March 2013.

crime and state-sponsored activities is often blurred in practice, with attribution being costly in terms of time and effort.[8]

Since there is no consensus on the threat landscape and there is a large diversity of political systems and cultures, there is no single institutional construction that can be identified as a role model for others. Various issues are, however, addressed in similar ways. What stands out, for instance, is that when nations define the roles and responsibilities of the armed forces vis-ą-vis civilian authorities in cyberspace, these are translated as literally as possible from the physical world. For example, the Dutch defence strategy for operating in cyberspace states that "[t]he three core tasks of the Defence organisation are leading for the armed forces' efforts in cyberspace."[9] When defining government responsibilities in cyberspace, states therefore generally start by adapting existing mandates and institutions.[10] Furthermore, there is general recognition of the need for a "comprehensive approach" to cyber security, in other words coordination between all stakeholders, and a need for cooperation between all relevant public, private and military entities. To improve cooperation, some countries like France and Australia have positioned the organization responsible for coordinating cyber policy at the highest level, directly under the prime minister or president. As ministries logically further their own organizational interests, be it the economy, human rights or security, this institutional construction allows for the balancing of higher order interests. An example would be defence or intelligence services advocating upstream data collection or keeping zero-day vulnerabilities unpatched for legitimate security reasons, while international economic or political repercussions might outweigh the security benefits.

Although the need for close cooperation between the armed forces and civilian authorities is often explicitly addressed in national security as well as national cyber security strategies, few countries are clear about the ways in which these intentions are to be realized. For instance, the French national cyber security strategy presents cyber defence as a civilian challenge, without mentioning the role of the armed forces.[11] Furthermore, although the armed forces are represented in the Information Systems Security Strategic Committee (*comité stratégique de la sécurité des systèmes d'information*), headed by the General Secretary for Defence and National Security, there is no further mention of the role the armed forces play in the response to high impact cyber attacks against critical infrastructure. Another example is the 2010 national security strategy of the United Kingdom which emphasises the "need [for] a whole-of-government approach to implementing this National Security Strategy."[12] Neither the national cyber security strategy nor the annual progress reports on the national security strategy and the national cyber security strategy, however, make any specific reference to cooperation between the armed forces and civilian cyber security authorities.

[8] Thomas Rid & Ben Buchanan, '*Attributing Cyber Attacks*', Journal of Strategic Studies, Volume 38, Issue 1-2, 2015.

[9] *The Defence Cyber Strategy*, Netherlands ministry of Defence, June 2012. Retrieved from: https://ccdcoe.org/strategies-policies.html [accessed March 2015].

[10] Ian Wallace, '*Five Guiding Principles for the Development of National Cyber Strategies*', Brookings Opinion, June 2014.

[11] *Information systems defence and security, France's strategy*, Office of the Prime Minister (2011), p. 21. Retrieved from http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf [accessed March 2015].

[12] *A Strong Britain in an Age of Uncertainty: The National Security Strategy 2010*, p. 34. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [accessed March 2015].

A common thread in Europe and several Asian countries is the limited role of the military in protecting critical infrastructure. This is understandable as most threats against national security in cyberspace will, at least during peace-time, be directed against civilian (public or private) infrastructure and will therefore have to be dealt with primarily by the organisations themselves, organisations responsible for sectoral oversight, and law enforcement agencies. Some nations have institutional and legal structures in place that allow for the assistance of the military in crisis management and incident response in case of a national emergency. In Europe, there seems to be consensus that these military capabilities should fall under civilian authority when deployed.[13] In many countries in Asia, however, a stronger and more coordinating role for the military does not seem controversial.[14] Nonetheless, in (cyber)crisis situations outside of an armed conflict, the role of the armed forces remains limited in most countries. National cyber security strategies indicate that in most countries the military have no formal responsibility at all, except in securing their own networks and as an eventual last resort if assistance is specifically requested by the civilian authorities. Japan seems to be the exception where paradoxically the armed forces have a very limited constitutional role. The Japanese National Cyber Security Strategy seems to give a leading role to the Self Defence forces in responding to cyber attacks against critical infrastructure, although the language is somewhat ambiguous.[15]

The emergence of a new policy area may lead to inter-agency fighting for as large a share as possible of newly allocated resources.[16] This can also take place within military organisations where there might be competition for resources between military intelligence and the various operational commands. Interagency rivalries can lead to unclear lines of command, often illustrated by the use of ambiguous language for the division of responsibilities. This vague use of language stands out when comparing national strategies and policy papers. In many countries, the division of responsibilities in crisis situations is not clear cut in official documents. Moreover, in situations where there is clear division of responsibilities, this has often not yet been tested in a real crisis situation. The current Dutch approach, for example, seems to be to bring together all the relevant stakeholders in a crisis situation and expect issues of command and responsibility to be resolved during the evolution of the crisis.[17]

However, in crisis situations, such vagueness will likely have a negative impact on the effectiveness of the response. The Estonian Cyber Security Strategy of 2014 recognises this problem and states that in order "to ensure the ability to provide national defence in cyberspace, the state's civilian and military resources must be able to be integrated into a functioning whole under the direction of civilian authorities as well as being interoperable with the capabilities of international partners."[18] Furthermore, to clarify such institutional issues and ensure that organisations are prepared when a crisis occurs, it is vital that nations conduct intensive training

[13] Luijf e.a. '*Organisational structures & considerations*, in 'National Cyber Security Framework Manual', p. 121.

[14] Authors' attendance at RSIS-Leiden University Centre for Terrorism and Counterterrorism (CTC) Roundtable on Civil-Military Relations in Cyberspace, Singapore, 18-19 November 2014.

[15] Japan Cyber Security Strategy, 2013, p. 42; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf [accessed March 2015].

[16] Luijf e.a, *Organisational structures and considerations*, in Klimburg e.a., 'National Cyber Security Framework Manual' (Tallinn 2012), p. 140.

[17] Dennis Broeders, '*Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*', Department of Sociology, Erasmus University of Rotterdam, 2014, p.46.

[18] *Estonian Cyber Security Strategy 2014-2017*, p 6; https://ccdcoe.org/strategies-policies.html [accessed March 2015].

and exercises with all stakeholders to get a more accurate understanding of the practical requirements in actual crisis situations.

Information-sharing between civilian and military or government and private actors is also considered to be crucial for crisis management and incident response. An important part of cyber defence, such as situation awareness, good threat intelligence analysis and building network resilience, takes place before the threat manifests itself as an attack. One institutional arrangement that facilitates information-sharing is the colocation of military and civilian Computer Emergency Response Teams (CERT's). This is, for instance, the case in France and Australia.[19] For example, the Australian Cyber Security Centre, which was established in November 2014, falls under the joint responsibility of the Attorney General and the Ministry of Defence. It is headed by a major general who commands the Department of Cyber and Information Security Directorate at Australia's Signals Intelligence Agency. It should be noted, however, that having a military officer as head of such a unit can convey a certain unwelcome signal to third (state) parties, in a region where military tensions should be carefully managed. Although certainly beneficial from an information sharing perspective, colocation could negatively impact on the perceived neutrality of government controlled CERT's.

When considering the role of the armed forces in cyber defence, it is important to also consider the distinction between the military and the intelligence sector. While the military often has a limited role in protecting national critical infrastructure outside of an armed conflict, the intelligence agencies play an increasingly important role in cyber security. In most countries, the technically proficient signals intelligence agencies have been tasked with cyber operations and these organisations are often military. The United Kingdom's Government Communications Headquarters (GCHQ) is one of the few signals agencies that is civilian and, in addition, also responsible for the government's CERT.[20] This is not an unusual construction and it allows for the efficient monitoring of networks for malware while also facilitating surveillance and espionage activities.[21] Intelligence agencies are responsible for the acquisition of data and information, and they execute covert operations that can encompass anything from sabotage to psychological operations.[22] This means accountability, transparency, and information-sharing with third parties are probably more complicated when intelligence organisations are involved instead of the military alone.

Regarding cooperation between (military) intelligence agencies and other public and private organisations, countries should recognise that the legitimate interests of these entities can vary greatly. For instance, the goal of a national CERT or a National Cyber Security Centre is to collect information on threats and vulnerabilities to inform stakeholders and provide solutions, whereas intelligence services may have a very different interest. They may instead require

[19] In France, the Network and Information Security Agency (ANSSI), an overarching inter-ministerial authority that falls under the responsibility of the prime minister, hosts the CERT or crisis management centre (COSSI). This is co-located with a military CERT that is a part of the Defence cyber unit, the CALID, that is in turn part of the military cyber command. See http://www.ssi.gouv.fr/. For the institutional arrangement in Australia. See: http://www.asd.gov.au/infosec/acsc.htm [accessed March 2015].

[20] See the official website at: http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx [accessed March 2015].

[21] While the military are bound by the internationally recognised legal cadres of humanitarian law, espionage is not constrained by any international legal framework.

[22] Stuxnet is the prime example of a cyber (sabotage) operation conducted by state actors. See Kim Zetter, '*Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*', Crown Publishers, New York 2014.

information on threats and specific weaknesses so that they can exploit them when the national need arises. Cyber security strategies and policies therefore need to recognise and clearly define these different security interests.[23] The practice of designating an overarching responsible cyber unit facilitates an executive decision when these interests clash. National policies, regulations and procedures should stipulate what information should be shared, how organisations should work together to address a specific threat or incident, and how organisations should process and disseminate information on threats and vulnerabilities as well as counter measures.

3. ENHANCING MILITARY COOPERATION ACROSS ASIA AND EUROPE

The challenges faced by nations when defining the role of the military regarding cyber security also have important international dimensions. Improving international cooperation between civilian and military entities and between international organisations should therefore strengthen the national security of individual states. This section therefore considers structures across Asia and the EU to enable better international military cooperation between the two regions for cyber related incidents. Given the widespread concern that a cyber incident, whether in the civilian or military domains, could cause tensions and unwanted escalation, makes efforts to improve international cooperation especially important. Additional mechanisms should be developed to enhance transparency, predictability, and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of cyber capabilities.[24] This is especially the case since military cooperation structures are currently at a relatively early stage of development. In terms of establishing cooperation, it is also important to consider that, as noted earlier, not all countries across these two regions share the same threat perception or strategic priorities. Historical context, domestic considerations and the wider geostrategic context in both regions remain significant factors. And while several of these findings may not be particularly surprising, with the requisite political willingness, there are several mutually beneficial opportunities for deeper cooperation that could be pursued as a starting point for longer term collaboration.

Improved mechanisms are important given (i) the nature of cyber threats; (ii) the growing interest in cyber capabilities that are difficult to control with arms control mechanisms; (iii) an increasing recognition by many states of cyber as another domain for military operations, and (iv) operations that are becoming increasingly dependent on the availability of a secure digital environment. While there is a great deal of institutional capacity within NATO and the EU, experts highlight that beyond this there is a lack of fixed structure or templates for international military cooperation. At this juncture, military-to-military cooperation on cyber related matters is somewhat limited, particularly since countries are at different stages of policy development, and common understanding (which experts cite as one of the most important factors for cooperation) is lacking in this area.[25] The EU Cyber Defence Policy Framework, which was adopted in November 2014, identifies the significance of international cooperation and states that there is a need to ensure dialogue with international partners, specifically NATO and other

[23] For the perils of informal information-sharing arrangements, see Ewen MacAskill, 'Ex MI6 Chief calls for new compact between internet firms and spy agencies', The Guardian, 20 January 2015.

[24] OSCE participating states in Permanent Council Decision No. 1039 decided to elaborate a set of draft CBMs to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

[25] Authors' attendance, RSIS-Leiden CTC Roundtable.

international organisations (in particular, it states that increased engagement should be sought within the framework of the OSCE and UN).[26] The European Defence Agency (EDA) and European External Action Service (EEAS) are therefore establishing a more extensive contact network and beginning to engage both at the bilateral level with third countries in Asia, such as India and China for example, as well as with regional organisations.[27] The 2013 Cyber Security Strategy of the EU also calls for increased engagement with key international partners and organisations and recommends that EU consultations should be designed and coordinated to add value to existing bilateral dialogues between EU Member states and third countries.[28]

This is especially significant for the Asia region, where interstate relations are complex. When considering European policies toward Asia, it is important to not just consider the role of the EU collectively but also EU Member states' national strategies and the complex relationship between the two.[29] Furthermore, general observations point out that while EU Member states "tend to break ranks in pursuit of national gain" across the world, the "multilevel complexity of relations between Europe and Asia is of a different order to the situations that exists in other regions".[30] Analysts highlight what seems to be a growing view in ASEAN that the EU has become overly anxious over China's rise and is consequently still neglecting to engage systematically with the rise of other Asian powers.[31] In Asia, ASEAN is central in a regional architecture that includes groupings such as the ASEAN Regional Forum (ARF), ASEAN +3, East Asia Summit, and the ASEAN Defence Ministers Meeting-Plus (ADMM-Plus). The ADMM and ADMM-Plus are the key defence forums within ASEAN that focus deliberately on practical cooperation. The ARF provides an important opportunity for dialogue and it has hosted several workshops on matters such as the use of proxy actors, cyber incident responses, and CBMs in cyberspace. A working draft on CBMs is under negotiation by ARF participants, including the EU, and it is hoped that an active contact list will be agreed soon. However, there is some criticism that this process has already taken over two years.[32] Furthermore, experts have voiced concern over the efficiency of such diplomatic channels in this region given the speed with which cyber incidents might occur and the fact that there can be some difficulty in establishing what falls within either the political or military realms.[33] For now, there does not seem to be extensive coordination between the dialogue at the ARF and the ADMM and, ideally, the work of the foreign affairs tracks on cyber related matters could complement that of defence.

While several statements calling for regional collaboration on cyber threats have been issued by defence ministers at previous ADMM meetings, discussions on stronger collaboration and the possible development of an "ASEAN master plan of security connectivity" do not seem to have extensively progressed.[34] The Network of ASEAN Defence and Security Institutions (NADI)

[26] Council of the European Union, EU Cyber Defence Policy Framework, 15585/14, 18 November 2014, p. 2. See also: related General Affairs Council conclusions, 25 June 2013.

[27] Neil Robinson, "EU cyber defence: a work in progress", European Union Institute for Security Studies, Brief Issue 10, March 2014, p. 4.

[28] Joint communication, *Cybersecurity Strategy of the European Union*, p. 15.

[29] Richard Youngs, "*Keeping EU-Asia Reengagement on Track*", Carnegie Europe, January 2015, p. 4.

[30] Ibid.

[31] Ibid.

[32] Authors' attendance, RSIS-Leiden CTC Roundtable.

[33] Ibid.

[34] *"ASEAN must tackle cyber security threat"*, New Straits Times, 31 May 2012. See also: IISS, *"New Forms Of Warfare - Cyber, UAV's and Emerging Threats: Dato'* Seri Dr Ahmad Zahid Hamidi", http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/fourth-plenary-session-1353/dato-seri-dr-ahmad-zahid-hamidi-b13b [accessed March 2015].

did hold a workshop on emerging cyber security challenges and responses in 2013 at which it tabled recommendations for consideration. NADI is a Track II forum that complements the ADMM and furnishes recommendations into the ADMM process by bringing defence officials and analysts together to discuss security matters that are sometimes deemed too sensitive for discussion at official Track I meetings.[35] While there is a close network of officials who regularly attend the ASEAN defence meetings and an evident shared focus on the concrete implementation of policies that rivals parallel negotiations between civilian ministries, there is still a greater need in both the ASEAN region and the wider Asia Pacific for enhanced CBMs and transparency measures such as further military-to-military engagements, dialogue, information sharing, joint exercises, official military-to-military contact points, and crisis communication procedures.

In both the EU and Asia, cyber defence is a national sovereign prerogative. Military cyber defence in the EU is currently considered to be at a relatively early stage of maturity.[36] Moreover, cyber defence capability varies greatly between the Member states - for example, a 2013 EDA-commissioned study found a complex and diverse picture regarding cyber defence capabilities within the 20 participating Member states.[37] The study further noted that the complex operational set up between the EDA, EEAS, General Secretariat of the EU Council and European Commission, and related EU agencies like the European Network and Information Security Agency (ENISA), the European Cybercrime Centre (EC3) and CERT-EU should be highlighted.[38]

Similarly, the Asia Pacific is a diverse region comprising countries that are at very different stages in terms of cyber technologies as well as strategy development and implementation. In addition, the institutional and operational structures of regional organisations, like the much smaller ASEAN Secretariat, are far more simplistic than those within the EU. Cyber defence capabilities vary significantly between countries across the region and given the sensitivities surrounding cyber security, in particular capabilities, it can be difficult to precisely ascertain the extent to which state actors have developed or acquired capabilities. In spite of this, increased military developments of operational cyber capabilities are expected.[39] The challenge lies not so much in an increase in military acquisition of capabilities, since states will seek to develop capabilities, but rather experts are also concerned about the current lack of military-to-military dialogue.[40] This is particularly pertinent given the strategic context of the Asia Pacific region where there are high national security sensitivities, unprecedented military modernisation and defence spending, on-going territorial and maritime disputes, uncertainty surrounding China as a regional military power and the United States' *'pivot'* towards Asia, as well as heightened concerns over North Korea. Non-state actors cause even further complication, and the growing

[35] Track II diplomacy generally refers to non-governmental, informal and unofficial contact and activities that can assist official actors by exploring solutions without the requirements of formal negotiation whereas Track I diplomacy can be defined as official, governmental diplomacy.

[36] European Defence Agency, "*Cyber Defence Fact Sheet*", www.eda.europea.eu [accessed March 2015].

[37] Ibid. EDA has 27 participating member states (all EU with exception of Denmark).

[38] Ibid. In general, EEAS leads third party (state or organisation) dialogues and cooperation. Although the EUMS and EDA have their own authorities to establish links with third parties, this is much more limited.

[39] Australian Strategic Policy Institute, "*Cyber Maturity in the Asia-Pacific Region 2014*", ASPI International Cyber Policy Centre, April 2014, p. 7.

[40] Authors' attendance, RSIS-Leiden CTC Roundtable.

levels of cybercrime in the region could cause further instability because of connections to espionage and military activities.[41]

In fact, current analyses identify that the most dynamic areas of Europe-Asia relations have recently come through extended bilateral efforts on both sides rather than on a region-to-region basis.[42] Such bilateral cooperation could be less problematic for militaries to develop, particularly since it might sometimes be easier to establish trust and when the relationship is based on national priorities, shared interests are often easier to identify.[43] In order to create an environment for cooperation in cyber defence, military experts argue that while these are sovereign decisions, sovereignty itself is not in fact the decisive factor - trust and shared interests are more powerful drivers when deciding on the degree of cooperation.[44] More recently, analysts further observe that cooperation efforts at the sub-regional level between like-minded groupings from Asia and Europe can sometimes allow for the embedding of practices that could then be extended to a regional level.[45] These observations also apply to cooperation efforts between groupings in Asia and Europe (or further afield) in cyber related matters. Although, some argue that while it is probable that like-minded communities can create CBM's and transparency mechanisms more easily, they are pessimistic when it comes to potential adversaries given, for instance, the visible difficulties of establishing such mechanisms in the U.S.-China working group.[46] Given these realities, states from Asia and Europe should concentrate on building better trust and coordinated cooperation at bilateral and regional levels that are mutually reinforcing.

Several additional mechanisms could be considered to enhance cooperation between Europe and the Asia Pacific region. For instance, Track I and Track II consultations and workshops can provide a venue for the exchange of opinions, military doctrine and strategies, national structures and best practice in crisis management or civilian missions. Such exchanges can enhance transparency and communication in order to build trust and common understanding as well as create informal networks and contact points. More particularly, if meetings were to be held more regularly, this would again allow for more enhanced trust and common understanding. For example, ARF participants took part in a table-top exercise in March 2014 to exchange details on national practices, and a roundtable on civil-military relations in cyberspace in November 2014 allowed for exchange of opinions and national strategies while also informally gathering a network of defence officials from across Asia and Europe.[47]

While multilateral MOUs could also be considered, Asian officials further suggest that international security and defence forums like, for instance, the Shangri-La and Seoul Defence dialogues, are helpful mechanisms to engage in dialogue on cyber defence.[48] At the Seoul

[41] James Lewis, "*Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*", prepared for the Lowy Institute MacArthur Asia Security Project, 2013, http://csis.org/files/publication/130307_cyber_Lowy.pdf, [accessed March 2015].

[42] Youngs, "Keeping EU-Asia Reengagement on Track", p. 7.

[43] Authors' attendance, RSIS-Leiden CTC Roundtable.

[44] Wolfgang Röhrig and Wg. Cdr. Rob Smeaton, "*Cyber Security and Cyber Defence in the European Union*", https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf, [accessed March 2015].

[45] Youngs, "Keeping EU-Asia Reengagement on Track", 19.

[46] Authors' attendance, RSIS-Leiden CTC Roundtable.

[47] ARF Workshop on Cyber CBMs, Kuala Lumpur, March 2014 & RSIS-Leiden CTC Roundtable, Singapore, November 2014.

[48] Authors' attendance, RSIS-Leiden CTC Roundtable.

Defence Dialogue in 2014, for example, over 20 countries discussed the military's role in cyber and a working group was established to promote pragmatic dialogue in order to enhance common understanding and ultimately, to assist in establishing structures for cooperation.[49] Singapore's Defence Minister recently echoed similar sentiments when urging enhanced collaboration through multilateral platforms like the Shangri-La Dialogue and ADMM-Plus grouping.[50]

The Multinational Capability Development Campaign (MCDC) has also been proffered as an opportunity for engagement since, although it is led by the U.S., it is regarded as a neutral platform operating at the unclassified level with less political constraints (Japan and South Korea are observers for example).[51]

Identifying and retaining cyber experts in the armed forces is also identified as a common problem in both the EU and across several countries in Asia, especially since this is a competitive market given the more profitable civilian domains. This is another area where collaborative exercises or discussions on best practices could be exchanged. In fact, the EU Cyber Security Strategy of 2013 suggests the EDA and Member states should collaborate on improving cyber defence training and exercise opportunities in the European and multinational context. The EU Cyber Defence Policy Framework further proposes the establishment of a cyber defence dialogue on training standards and certification with third countries and international organisations.[52] At national level, a number of states have been running bilateral or small exercises with other like-minded nations.[53]

4. CONCLUSION

Due to differing threat perceptions and a large diversity of political systems and cultures across Asia and Europe, the institutional embedding of roles and responsibilities in the cyber domain is generally based on specific national political and organizational traditions and processes. Consequently, there is no single institutional construction that can be identified as a model for others. Although countries recognise that the government shares responsibility for the protection of critical infrastructure against cyber threats, in most cases the military only play a limited role. Often the exact roles that different ministries and the military should play during crisis and incident response are not clearly formulated in the cyber strategy and policy documents. In so far as there are clear institutional arrangements, these are generally still untested given that (actual) cyber crises involving critical infrastructure in Europa and Asia have been have as of yet only occurred sporadically. Carrying out exercises would certainly contribute to the clarification of the roles of different stakeholders.

Civil-military relations can be improved through different mechanisms. Clearly defined procedures facilitate information-sharing between different parties and stakeholders. The exact

[49] Seoul Defense Dialogue 2014, http://sdd.mnd.go.kr/user/boardList.action?boardId=O_63480&siteId=sdd&page=1&search=&column=&boardType=02&listType=&id=sdd_060300000000&parent=&boardSeq=O_63492&command=albumView&chkBoxSeq=&chkBoxId=&chkBoxPos=&chkBoxDepth=&chkBoxFamSeq=&warningYn=N&categoryId=&categoryDepth=.

[50] Jermyn Chow, "*Ng Eng Hen: Deeper issues beyond the ISIS threat*", Straits Times, 27 January 2015.

[51] Authors' attendance, RSIS-Leiden CTC Roundtable.

[52] *EU Cyber Defence Policy Framework*, p. 11.

[53] Röhrig and Smeaton, "*Cyber Security and Cyber Defence*".

role and responsibility of the intelligence agency in the national cyber landscape is crucial in many countries and will determine how information is shared between public and private actors, as well as how networks of trust and questions relating to transparency can be addressed. States must be aware that all institutional arrangements, such as military commanders for civilian cyber centres, as well as the wording of their cyber security strategies, not only serve a national purpose but also have a strong declaratory function vis-a-vis other state parties.

Given the international nature of the cyber threat, it is not only important to improve mechanisms for dialogue, cooperation, and transparency within regional structures such as the EU and ASEAN but also between the two regions. States from Asia and Europe should therefore concentrate on building better trust and coordinated cooperation, where appropriate, at bilateral and regional levels that is mutually reinforcing. Moreover, in situations where interstate tensions are prevalent, improved military-to-military communication is vital. In this regard international meetings, like the civil-military Singapore roundtable, held in November 2014 are useful to build trust and create understanding between different policy makers.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence*

Geoffrey S. DeWeese
U.S. Army
U.S. Strategic Command
Offutt Air Force Base, Nebraska, USA

Abstract: As the potential for disastrous consequences from cyber threats increases in prevalence, the speed which such cyber threats can occur presents new challenges to understandings of self-defense. This paper first examines the cyber threats nations could face. It next looks at existing concepts of self-defense with particular focus on anticipatory and preemptive self-defense, and then moves to a review of the underlying criteria which govern the right to resort to such actions. As will be shown, definitions for anticipatory and preemptive self-defense are less useful than an understanding of the actual criteria that must be met to justify their use. These criteria include necessity and proportionality, and for anticipatory and preemptive actions, imminence. The paper will turn this review to the cyber context, first examining how cyber operations are conducted, and then applying the self-defense criteria to the cyber domain. As will be shown, the most critical legal challenge in this analysis will be the determination of an imminent threat. Imminence in the cyber domain must not be tied to a strict temporal analysis, but should accommodate a broader window of opportunity approach, which in turn must give consideration to the likelihood that a victim State may not always know the intent of an adversary who implants malicious malware on the victim State's critical infrastructure. Using a hypothetical case, the paper will evaluate potential decision making for a State facing a potential cyber threat. In conclusion, the paper will show that an understanding of the process for determining a right to anticipatory or preemptive self-defense must be considered by a cyber actor conducting cyber operations on a potential adversary's systems to help ensure such actors do not inadvertently give their adversary a reasonable basis to determine that an attack is imminent.

Keywords: *anticipatory and preemptive self-defense, imminence*

* The views and opinions expressed in this article are those of the author alone and do not necessarily reflect those of the United States Department of Defense, the United States Army, the United States Strategic Command, or any other United States government agency.

1. INTRODUCTION

In October 2012, former U.S. Secretary of Defense Leon Panetta warned in a speech in New York City that "[a] cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11."[1] Secretary Panetta pointed to increasing threats such as the Distributed Denial of Service (DDOS) attacks on the U.S. financial sector and the deployment of the Shamoon virus which essentially destroyed 30,000 computers belonging to the Saudi Arabian Aramco oil company.[2] He warned that "foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country."[3] In some cases, he noted, they have actually gained access to such systems, and "they are seeking to create advanced tools to attack these systems."[4] The result, he concluded ominously, "could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[5] Echoing his remarks, the U.S. Chairman of the Joint Chiefs of Staff, General Martin Dempsey, called cyber "one of the most serious threats to our national security," noting that "[w]e now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."[6] As a result, General Dempsey concluded, "our military must be ready to defend the nation and to do so at network speed."[7]

The United States has made clear that it will treat cyber attacks in the same manner as conventional attacks. The U.S International Strategy For Cyberspace states that "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[8] At a speech at U.S. Cyber Command in September 2012, then Legal Advisor to the U.S. Department of State, Harold Koh, elaborated on the U.S. position stating: "A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or an imminent threat thereof."[9]

[1] Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136. (*hereinafter* Panetta Speech).

[2] *Id*. Regarding the financial sector attacks, see Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST, 21 Sept. 2012, http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html. Regarding the Saudi Aramco attack, *see* Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

[3] Panetta Speech, *supra* at 1.

[4] *Id.*

[5] *Id*.

[6] Gen. Dempsey's Remarks at the Brookings Institute, "Defending the Nation at Network Speed", 27 July 2013, http://www.jcs.mil/Media/Speeches/tabid/3890/Article/5054/gen-dempseys-remarks-at-the-brookings-institute-defending-the-nation-at-network.aspx (*hereinafter* Dempsey Speech). *See also* RICHARD A. CLARKE AND ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 31(2010) ("Cyber war happens at the speed of light").

[7] Dempsey Speech, *supra* at 6.

[8] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (*hereinafter* Int'l Strategy for Cyberspace).

[9] Harold Koh on International Law in Cyberspace, 18 September 2012, http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ (*hereinafter* Koh Speech).

Given the cyber threats such as those laid out by Secretary Panetta above, how can a nation defend against potential destructive acts which could be launched at "network speed"? This paper will review the right to national self-defense under international law, with a particular focus on anticipatory and preemptive self-defense and the criterion of imminence. Given the numerous perspectives which inform the discussion, this first section will present both a general overview for the reader less familiar with the debates, and lay a foundation for how these principles will be applied in this paper. Using this foundation, this paper will next overlay these principles within the cyber domain and demonstrate how the principle of imminence creates greater complexity for cyberspace. A hypothetical case applying these principles in cyber will conclude the paper.

2. SELF-DEFENSE

Self-Defense Generally

The UN Charter prohibits the "threat or use of force" by one State against another in Article 2(4).[10] However, Article 51 explicitly recognizes the "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[11] On its face, this language would appear to require that a State must first be attacked prior to resorting to self-defense.[12]

Despite the wording of Article 51, many States interpret the language as more permissive and inclusive of anticipatory actions as a customary international law norm.[13] Under this view, a State is "not required to absorb the first hit before it can resort to the use of force in self-defense to repel an imminent attack."[14] Indeed, even those who advocate a strict interpretation of Article 51 recognize that history is replete with instances where States have resorted to anticipatory actions in self-defense.[15] Of these, the Caroline incident is the most often cited.[16]

[10] U.N. Charter art. 2, para. 4. This prohibition is considered customary international law and applicable to all nations, whether signatories or not. YORAM DINSTEIN, WAR AGGRESSION AND SELF-DEFENCE 95 (5th ed. 2011).

[11] U.N. Charter art. 51.

[12] *See e.g*. W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 A.J.I.L. 525,525 (2006); DINSTEIN *supra* note 10 at 193; LAW OF ARMED CONFLICT DESKBOOK 34 (WILLIAM J. JOHNSON & DAVID H. LEE, editors, 2014) (*hereinafter* LOAC DESKBOOK).

[13] LOAC DESKBOOK, *supra* note 12, at 34-35. *But see* DINSTEIN, *supra* note 10, at 197 stating, "The idea that one can go beyond the text of Article 51 and find support for a broad concept of anticipatory or preemptive self-defence in customary international law (which, supposedly, Members of the United Nations did not 'forfeit') is counter-factual."

[14] *Id*.at 37. *See also* Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 535 (2003) ("It would be absurd to suggest that international law requires a State to 'take the first hit' when it could effectively defend itself by acting preemptively.").

[15] DINSTEIN, *supra* note 10 at 195.

[16] *See generally*, LOAC DESKBOOK, *supra* note 12 at 37-38; David A. Sadoff, A Question of Determinacy: The Legal Status of Anticipatory Self-Defense, 40 GEO. J. INT'L L. 523, 535-37 (2009); John J. Merriam, *Natural Law and Self-Defense*, 206 MIL. L. REV. 43, 59-61 (2010); Schmitt, *supra*, note 14, at 529-530; Noura S. Erakat, *New Imminence in the Time of Obama: The Impact of Targeted Killings on the Law of Self-Defense*, 56 ARIZ. L. REV. 195, 203-204 (2014); MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 74-75 (4th ed., 2006).

In 1837 British forces operating out of Canada crossed into New York and seized the *Caroline* (a steamer which had been used by rebels in Canada and their American supporters), set it on fire, and sent it plummeting to its doom over Niagara Falls.[17] In 1842 U.S. Secretary of State Daniel Webster responded to the British claim that the action was appropriate self-defense.[18] Webster stated that "while it is admitted that exceptions growing out of the great law of self-defence do exist, those exceptions should be confined to cases in which the 'necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'"[19]

The extent of this "just" right is unsettled. Michael Walzer described the range as such: "Imagine a spectrum of anticipation: at one end is Webster's reflex, necessary and determined; at the other end is preventive war, an attack that responds to a distant danger, a matter of foresight and free choice."[20] Following is an overview of four views of this spectrum: interceptive, anticipatory, preemptive, and preventive. These are not clearly defined, and the differences have been called "confounding" as "[t]here appears to be no clearly, uniformly adopted nomenclature for describing the various kinds of self-defensive strikes a State might launch in the face of an as-yet-unrealized security threat."[21] But they predominate any discussion of self-defense.

Interceptive Self-Defense

Interceptive self-defense, according to Dinstein, still falls within a strict reading of Article 51.[22] In essence, interceptive self-defense is a "reaction to an event that has already begun to happen (even if it has not yet fully developed in its consequences)."[23] Under Dinstein's view, this would include any use of force to respond to an attack that has commenced, though it has not yet reached the defending State's borders. In other words, the attack, while underway, is intercepted prior to it reaching its target.[24] As an example of interceptive self-defense, Dinstein offers the scenario where the U.S. was able to destroy the Japanese force that was *en route* to the infamous attack on Pearl Harbor. While the Japanese would not have yet launched a single Zero, the fact that the fleet was underway with the mission to attack meant that the overall attack had begun, and it could be intercepted prior to it achieving its objective.[25] However, "[t] raining, war-gaming and advance preparations do not cross the red line of an armed attack" and Dinstein argues they therefore do not give recourse to self-defense under this reading of Article 51.[26]

Anticipatory and Preemptive Self-Defense

Trying to establish an agreed upon definition for anticipatory and preemptive self-defense is, as previously noted, "confounding,"[27] but the U.S. Army's Law of Armed Conflict Deskbook (hereinafter LOAC Deskbook) definition is a good place to begin. Anticipatory self-defense

[17] Hunter William, *Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, British-American Diplomacy, The Caroline Case*, at http://avalon.law.yale.edu/19th _centrury/br-1842d.asp [hereinafter Avalon Project, Caroline Case].

[18] *See* Schmitt, *supra* note 14, at 529-30.

[19] Letter of Daniel Webster to Lord Ashburton, (August 6, 1842), Avalon Project, Caroline Case *supra* note 17.

[20] WALZER, *supra* note 16, at 75.

[21] SADOFF, *supra* note 16 at 529.

[22] DINSTEIN *supra* note 10 at 204.

[23] *Id*. at 203.

[24] *Id*. at 203-205. *See also* Sadoff, supra note 16 at 529.

[25] DINSTEIN, *supra* note 10 at 203-04.

[26] *Id*. at 204.

[27] *See supra* note 21 and accompany text.

there is defined simply as "using force in anticipation of an imminent armed attack" while preemptive self-defense is viewed as a subset of this broader concept.[28] The "Bush Doctrine", laid out in the 2002 National Security Strategy,[29] is offered as an example of preemptive self-defense.[30] The Bush Doctrine maintains, "The United States has long maintained the option of preemptive actions to counter a sufficient threat to our national security. The greater the threat, the greater the risk is of inaction – and the more compelling the case for taking anticipatory action to defend ourselves."[31]

Gill and Ducheine define anticipatory self-defense as "defensive measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future."[32] In their view, this term, and its definition, is synonymous with preemptive self-defense, rather than a subset as laid out in the LOAC Deskbook.

Dinstein notes that the "outlines of each term may vary, but their common denominator is that they are all conjectural."[33] David Sadoff describes both as part of a spectrum similar to Walzer's[34] where the dividing line is "based on the real or perceived timing of the threat posed by an aggressor State."[35] This temporal distinction then is the primary difference between anticipatory and preemptive self-defense – how imminent is the threat? Sadoff defines anticipatory self-defense as using force "in 'anticipation' of an attack when a State has manifested its capability and intent to attack imminently."[36] Preemptive self-defense then, according to Sadoff, "stems from a fear that in the near future, though not in any immediate sense, a State may become an armed target of an aggressor State."

This is echoed by Michael Reisman who states, "those contemplating [anticipatory self-defense] can point to a palpable and imminent threat."[37] Key to this articulation is "palpable evidence of an imminent attack."[38] Preemptive self-defense, however, "can point only to a possibility among a range of other possibilities, a contingency."[39] It would appear therefore that the key difference between the two (for those who, unlike Gill and Ducheine, see a difference) lies in the degree of conjecture as to the imminence of the threat which will be defended against, with preemptive requiring the greater degree of conjecture.

[28] *See* LOAC DESKBOOK, *supra* note 12, at 37-38.

[29] Of course, the 2002 National Security Strategy never refers to a "Bush Doctrine", but that name has become synonymous with the policy that is laid out. See DINSTEIN, supra note 10 at 194-95.

[30] *See* LOAC DESKBOOK, *supra* note 12, at 38.

[31] The National Security Strategy of the United States 15 (Sept 2002) (hereinafter 2002 NSS). Note that it intermingles the terms anticipatory and preemptive. Dinstein notes that the Bush Doctrine "was intended to push the envelope by claiming a right to counter threats – before they morph into concrete action." DINSTEIN, *supra* note 10, at 195. This seems to fall in line with the LOAC Deskbook view of preemptive self-defense as a more expansive subset of anticipatory self-defense. It is interesting to note, however, that Dinstein also stakes the position that as applied, the Iraq invasion of 2003 was not in fact an application of the Bush Doctrine as laid out in the 2002 NSS.

[32] Terry D. Gill and Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INTERNATIONAL LAW STUDIES 438, 452-53 (2013).

[33] DINSTEIN, *supra* note 10, at 195. Dinstein also includes preventive self-defense in this consideration.

[34] *See supra*, note 20.

[35] Sadoff, *supra* note 16, at 530.

[36] *Id*.

[37] Reisman & Armstrong, *supra* note 12, at 526.

[38] *Id*.

[39] *Id*.

Preventive Self-Defense

The LOAC Deskbook differentiates preventive self-defense from anticipatory (and preemptive) self-defense, defining preventive actions as those "employed to counter non-imminent threats," and bluntly declares such a theory to be "illegal under international law."[40] While similar in some respects to preemptive self-defense, preventive self-defense can be distinguished by a much broader temporal range – "preventive self-defense operates over a longer time horizon (even a matter of years)" than does preemptive self-defense.[41] It is a response to "an inchoate or potential threat of attack at some indeterminate point in the future."[42]

Preventive self-defense therefore does not require a current, definitive threat, just the possibility of a threat at some point in the future. Michael Walzer puts it this way: "Preventive war presupposes some standard against which danger is to be measured. That standard does not exist, as it were, on the ground; it has nothing to do with the immediate security of boundaries. It exists in the mind's eye, in the idea of a balance of power…."[43]

Summary

Interceptive and preventive self-defense do not require a threat be imminent, because in interceptive, the threat is already commenced, and in preventive the threat is merely a potential and distant threat. Between these two are anticipatory and preemptive self-defense, both which require a consideration of imminence. These will be the primary focus of the rest of this paper. To better understand these concepts, it is useful to turn to an examination of the underlying principles of self-defense.

3. NECESSITY, PROPORTIONALITY, AND IMMINENCE

Necessity and Proportionality

Two principles underlay the resort to self-defense under international law: necessity and proportionality.[44] Necessity requires that the force being used is "needed to successfully repel an imminent armed attack or defeat one that is underway."[45] In other words, other options would not be sufficient.[46] Importantly, necessity is a subjective standard, which "is judged from the perspective of the victim State," though such perspective must be reasonable based on the totality of the circumstances.[47] Next, proportionality addresses the level of force that can be used to respond, once a right to the resort to force is determined.[48] It limits the "scale, scope,

[40] LOAC DESKBOOK, *supra* note 12, at 39.

[41] Sadoff, *surpa* note 16, at 532 n. 36.

[42] GILL AND DUCHEINE, *supra* note 32, at 453.

[43] WALZER, *supra* note 16, at 76.

[44] *See generally*, Sadoff, *supra* note 16, at 526, LOAC HANDBOOK, *supra* note 12, at 35, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 61 (Michael Schmitt, gen. ed., 2013) (*hereinafter* TALLINN MANUAL), DINSTEIN, *supra* note 10, at 607. Dinstein further points to repeated pronouncements by the International Court of Justice in the Advisory Opinion on the *Legality of the threat or use of Nuclear Weapons*, and its Judgments in the *Oil Platform* case and *Armed Activities* case, which all identify necessity and proportionality as prerequisites for the resort to self-defense. DINSTEIN, *supra* note 10, at 607.

[45] TALLINN MANUAL, *supra* note 42, at 62.

[46] *See id*.

[47] *See id*.

[48] *See id*.

duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defence."[49] Therefore, a State must determine the necessity of acting in self-defense, and then, may only respond proportionally to the nature of the threat it is faced with.

Imminence

For anticipatory and preemptive self-defense the key to the determination of necessity is imminence. In fact, there is support for pulling imminence from under necessity and considering it as a third criterion for self-defense, alongside necessity and proportionality.[50] Clearly when an attack is actually occurring, imminence is a non-issue.[51] While both anticipatory and preemptive self-defense reference imminence, preemptive self-defense has the more expansive view of the concept.[52] The Bush Doctrine acknowledged the traditional legal requirement of imminent threats yet concluded this was no longer sufficient, stating that "[w]e must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries."[53] Even here, however, the focus is on adapting imminence, not discarding it.

This broader approach to imminence is well argued by Michael Schmitt. He notes in contrast to the narrow Webster view,[54] that "[w]hile a restrictive construction [of imminence] may have made sense in the nineteenth century, the nature of warfare has evolved dramatically since then."[55] Given that, "in the twenty-first century, the means of warfare are such that defeat, or at least a devastating blow, can occur almost instantaneously," Schmitt argues that "restrictive approaches to immanency run counter to the purposes animating the right of self-defense."[56]

Perhaps the most reasonable explanation for how to interpret imminence as it spreads from the "Webster's reflex"[57] to the less tangible forms in the Bush Doctrine[58] is the window of opportunity analogy. As expressed in the Tallinn Manual, the imminence criterion is met when an adversary State is "clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts. In other words, it may act anticipatorily only during the last window of opportunity."[59] The Tallinn Manual continues:

> This window may present itself immediately before the attack in question, or, in some cases, long before it occurs. The critical question is not the temporal proximity of the anticipatory defensive action to the prospective

[49] *Id*. Dinstein applies a subjective reasonableness standard to this determination similar to the one the TALLINN MANUAL applied to necessity. *See* DINSTEIN *supra* note 10, at 232-33. Reasonableness, it seems, applies across the board when looking at subjective determinations.

[50] *See generally* Schmitt, *supra* note 14, at 529-536, TALLINN MANUAL, *supra* note 45, at 63-66. In a memo to the British Prime Minister in July 2002, the British Attorney General, Lord Goldsmith, also listed imminence as a third, equal factor along with necessity and proportionality. "Force may be used in self-defense if: (a) there is an actual or imminent armed attack; (b) use of force is necessary i.e. the only means of preventing an attack; (c) the force used is proportionate." Attorney General Memo to the Prime Minister, http://www.iraqinquiry.org.uk/media/46499/Goldsmith-note-to-PM-30July2002.pdf.

[51] Thus Dinstein, who opposes the ideas of anticipatory or preemptive self-defense, defines necessity in terms of an action that has already occurred with no reference to one that is imminent. *See* DINSTEIN *supra* note 10, at 231.

[52] *See* LOAC HANDBOOK, *supra* note 12 at 38.

[53] *Id*.

[54] *See supra*, note 19, and accompanying text.

[55] Schmitt, *supra* note 14, at 534.

[56] *Id*.

[57] *See supra*, note 20, and accompanying text.

[58] *See supra*, notes 29-31, and accompanying text.

[59] TALLINN MANUAL, *supra* note 45, at 64-65.

> armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts.[60]

Similarly, Schmitt argued that "maturation of the right to self-defense is relative. For instance, as defensive options narrow or become less likely to succeed with the passage of time, the acceptability of preemptive action grows."[61]

Summary

Setting aside the vagrancies of which term one places on concepts of self-defense, the underlying requirements become clearer. Any action in self-defense first requires that it be against an action rising to the level of an armed attack. It must be necessary to take such defensive action, and the means used to respond must be proportionate to the threat. Further, for self-defense of an anticipatory or preemptive nature, the armed attack need not be underway or have already struck, but it must be imminent. Imminence may be based on a determination as to when the last window of opportunities to mount an effective defense.[62]

4. CYBER OPERATIONS AND SELF-DEFENSE

Cyber Operations

Understanding how cyber operations work is key to putting them in the context of a potential attack. Part of any cyber operation involves first probing, then gaining access to targeted networks. This has been referred to as the process of identifying key cyber terrain.[63] Through this process, "a network defender knows where to focus his energy to prevent penetration and an attacker can select a target within a network that provides maximum potential for success."[64] For the attacker, it is noted that "[o]ften, cyber terrain cannot be observed until it is accessed, so attackers are forced to engage in a constant process of reassessment of key terrain as they progress deeper into a network."[65] Further it is noted that, "[a] careful analysis of avenues of approach, observation points, and fields of fire can provide an attacker with a complete view of his or her options at each stage of the attack."[66]

[60] *Id*. at 65.

[61] Schmitt, *supra* note 14, at 534.

[62] Imminence must be distinguished from immediacy. Immediacy is the requirement that any action in self-defense be reasonably close in time to the armed attack which gave rise to the right. *See* DINSTEIN *supra* note 10, at 230-31. A response that is not reasonably proximate to the initial armed attack would instead qualify as retaliation. See TALLINN MANUAL, *supra* note 44, at 66. Since immediacy relates to the response *after* an armed attack, it is not central to considerations of anticipatory or preemptive self-defense and is not addressed in depth here. *See also* Gill & Ducheine, *supra* note 32 at 451, arguing that immediacy "relates to the distinction between self-defense, which is a recognized legal basis for the use of force, and armed reprisal, which is unlawful under contemporary international law." However, Gill and Ducheine appear to tie immediacy and imminence together as one concept. They note regarding immediacy, "[t]he important point is that self-defense is exercised within a reasonable timeframe in response to an ongoing attack or, … a clear threat of attack in the proximate future." *Id.* This paper follows the Tallinn Manual's view of these as distinct concepts, rather than one. *See* TALLINN MANUAL, *supra* note 44 at 63-66.

[63] David Raymond, et al, *Key Terrain in Cyberspace: Seeking the High Ground, in* 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 287 (P. Brangetto, et al, ed, 2014) Raymond, et al, define cyber terrain generally as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace." *Id*. at 290.

[64] *Id*. at 294.

[65] *Id*. at 298.

[66] *Id*.

This process has also been described as cyber maneuver[67] which was defined as "the application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors."[68] While in the kinetic world, maneuver would involve the actual movement of military forces, in the cyber context, it involves using code to achieve its purpose.[69] In doing this, "[c]yber maneuver leverages positioning in the cyberspace domain …. It is used to apply force, deny operation of or gain access to key information stores or strategically valuable systems."[70] One aspect of cyber maneuver is "Positional Maneuver" defined as "the process of capturing or compromising key physical or logical nodes in the information environment which can then be leveraged during follow-on operations."[71] The probable use of cyber operations by Israel to disable Syrian air defense systems prior to a 2007 Israeli air attack on a suspected nuclear power plant in Syria is offered as an example of this type of maneuver.[72] In that example, Israeli aircraft were able to fly into Syrian airspace without detection and achieve their objective and destroy the plant.[73] "The use of positional maneuver prior to the initiation of actual kinetic combat operations set them up for success and illustrates the potential decisive nature of this form of cyber maneuver, especially at the tactical and operational levels of war."[74]

These descriptions of cyber operations appear to describe the type of activity that Secretary Panetta warned about, that cyber actors are probing key cyber infrastructure controlling chemical, electrical and water plants, as well as transportation networks, and that they aren't just probing, but in some cases have gained access to such networks.[75] While the targets Secretary Panetta described may raise additional law of armed conflict targeting concerns, from a purely doctrinal perspective, these actions appear to be quintessential in cyber operations.

Necessity

When making a determination of necessity, States are required to first examine alternative courses of action prior to responding with a use of force.[76] Only "when measures falling short of a use of force cannot alone reasonably be expected to defeat an armed attack and prevent subsequent ones, [then] cyber and kinetic operations at the level of a use of force are permissible under the law of self-defense."[77] This determination, as noted, previously "is judged from the perspective of the victim State. The determination of necessity must be reasonable in the attendant circumstances."[78]

Imminence

The U.S. position, clearly enunciated in the Koh Speech, is that the inherent right to self-defense in cyberspace applies to imminent cyber threats of armed attack in the same degree as kinetic attacks.[79] The Tallinn Manual also took the position that self-defense in cyberspace

[67] Scott Applegate, *The Principle of Maneuver in Cyber Operations, in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 183 (C. Czosseck et al, ed 2012).

[68] *Id.* at 185.

[69] *Id*.

[70] *Id*. at 186.

[71] *Id*. at 189.

[72] *Id*.

[73] *Id*.

[74] *Id*. See also CLARKE & KNAKE, *supra* note 6, at 4-8.

[75] *See supra* notes 3-4 and accompanying text.

[76] TALLINN MANUAL, *supra* note 44, at 62.

[77] *Id*.

[78] *Id*.

[79] Koh Speech, *supra*, note 9.

could not be limited to only those cases where an armed attack had occurred or where one was already launched because "[t]he speed of cyber operations would usually preclude them from falling into [these] categories."[80] With this statement, the Tallinn Manual appears to endorse the potential of cyber threats at "network speed."[81] Given the speed of cyber, what qualifies as an imminent threat in cyberspace?

The concept of imminence as a purely temporal measurement is untenable in cyberspace where the click of a mouse could potentially launch an instantaneous cyber attack which could cause great damage.[82] Rather, the "window of opportunity" view presents a much stronger basis on which to gage defensive actions against threats. As already discussed, the Tallinn Manual clearly identifies this as being the point at which a failure to act may render a State unable to defend itself when the attack actually occurs.[83] The Tallinn Manual uses the example of a logic bomb inserted into a system to evaluate how imminence could apply in the cyber context.[84] "The insertion," the Tallinn Manual states, "will qualify as an imminent armed attack if the specified conditions for activation are likely to occur."[85] The challenge, of course, is determining what the specified conditions are, something that may not be immediately apparent. The Tallinn Manual attempts to differentiate this from remotely activated malware.[86] Only if the initiator actually decides to activate the remotely controlled malware, would the attack become imminent.[87] The problem is that whether faced with a logic bomb or a remotely activated malware, the victim State will not necessarily know when the attack would be initiated. The Tallinn Manual acknowledges this, noting "it will often be difficult to make the distinction in practice."[88] This is small help to the leaders who will have to make this determination, though such leaders may find comfort knowing the standard by which a State must make this determination is one of reasonableness, based on an assessment of the facts known to the victim State.[89]

Proportionality

Proportionality does not directly play into a determination of the right to anticipatory or preemptive self-defense, as the means of self-defense must be predicated on the determination that self-defense is first necessary. However, it is useful to note that within the cyber context, the proportionality of the response is not limited to purely a cyber response. As the Tallinn Manual makes clear, "there is no requirement that the defensive force be of the same nature as that constituting the armed attack. Therefore a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa."[90]

[80] TALLINN MANUAL, *supra* note 44, at 64.

[81] *See* Dempsey Speech, *supra* note 6.

[82] *See supra*, note 6, and accompanying text.

[83] *See supra* notes 59-60 and accompany text.

[84] TALLINN MANUAL, *supra* note 44, at 65.

[85] *Id*.

[86] *Id*.

[87] *Id*.

[88] *Id*.

[89] *Id*.

[90] *Id*. at 63.

5. APPLYING THE ANALYSIS – A HYPOTHETICAL CASE

Background

A hypothetical example may assist in evaluating the challenge States will be confronted with when putting principles of anticipatory and preemptive self-defense into practice. Recall the discussion of the Israeli cyber operation (the cyber maneuver) as part of the kinetic strike attack on the Syrian suspected nuclear plant discussed above.[91] Using that example as a baseline, assume a cyber defender in Brownland found evidence of a malicious code in the air defense systems. His discovery raises serious concerns and leads to a larger search on the networks. After extensive work, Brownland begins to piece together two facts – their computer system is at risk, which puts their entire air defense network at risk, and the evidence supports their conclusion that it was Greyland who was behind the exploit. Greyland is an adversary of Brownland. While comfortable with the factual basis for attribution to Greyland, Brownland does not have any intelligence available that provides any indication on what Greyland's plans are for the use of this malware. Looking at these facts, Brownland must determine if they are facing a potential Cyber Pearl Harbor,[92] where Greyland could shut down their defenses at a moment's notice and launch a devastating strike.

Application of Necessity

Brownland first must look at its options. It could raise the issue to the Security Council, or confront Greyland directly. However, doing this would alert Greyland to their knowledge and would deprive Brownland of the one advantage they have – the chance to eliminate the threat without giving their adversary a chance to use it. The best option would be for Brownland to simply overcome the code and remove it. This would be ideal, but Brownland would have to consider that they may not be able to remove it all or remove it swiftly enough. There may be technical challenges. Additionally, while this may eventually defeat the malware, they could reasonably conclude that if Greyland inserted the code, they may become aware of Brownland's efforts and this may prompt Greyland to activate the implanted code and shut down the air defense networks early, and possibly launch air attack. Thus, having reasonably ruled out other options, Brownland may find it necessary to resort to forceful self-defensive measures.

Determination of Imminence

Having determined that a use of force may be necessary to ensure national self-defense, Brownland would have to determine if the armed attack was imminent. Under these conditions, Brownland has no direct evidence of a temporal threat; they are as of yet unsure what the qualifying condition for activating the malware are. However, using the last window of opportunity analysis, they could reasonably deduce from the circumstances that they must act quickly or they could lose any strategic advantage in preventing a Greyland attack. Consulting the Tallinn Manual for guidance, they may find themselves unsure if they have an international legal basis to rely upon. The Tallinn Manual, they may note, would seem to require Brownland to have knowledge of Greyland's intent to activate the code, and only then would Brownland have legal justification to make the determination of imminence.[93] However, Brownland may determine that the window of opportunity for action is small, and that a failure to act quickly

[91] *See supra*, notes 72-73, and accompanying text.

[92] *See supra*, note 5, and accompanying text.

[93] *See supra*, notes 84-88, and accompanying text.

could reasonably result in their being unable to defend themselves effectively when (or even if) the malware is activated.[94] Under these facts, having their air defense system, a critical function of their defense infrastructure, "pwned"[95] by an adversary arguably justifies a determination of imminence given that the malware is present at that moment, and that it could be activated at any time. The threat is imminent, even if it is unclear if the intent to initiate the threat is. Their window to take action is narrow, and Brownland could find solace knowing that in the end, the determination of imminence is based on the reasonableness of the victim State, given the facts known to it at the time.[96]

Finding a Proportionate Response

Finally, Brownland, having determined it faced an imminent armed attack and that a use of force was necessary in self-defense, would have to determine what a proportionate response would be. Its actions would be limited in scale, scope duration and intensity to that needed to address the threat, but this would not be limited to only cyber actions.[97] Kinetic options could be employed, with the requirement that they must be directly focused on the purpose of self-defense against the threat.

6. CONLCUSION

This review of the right to national self-defense in light of the increasing threats in cyberspace demonstrates two things. First, it shows that existing norms of international law provide a sufficient guide to address the emerging threats in cyberspace. Self-defense, to include anticipatory and preemptive self-defense, can be applied against cyber threats in a similar manner to kinetic threats. Secondly, however, it demonstrates that while acknowledging the right to self-defense against imminent cyber threats is reasonable and justified, putting a measure on how to determine imminence against threats in cyberspace presents challenges which States have not previously confronted from conventional threats. Finally, it shows that cyber operations in an adversary's networks to maneuver to key cyber terrain may, if detected, cause the adversary to reasonably conclude that an attack is imminent. Since such cyber maneuver usually will occur well in advance of potential hostilities, it is critical that States carefully consider the ramifications of such actions and the possibility that such actions will be misconstrued as evidence of an imminent attack, resulting in the adversary launching its own defensive action in an anticipatory fashion.

ACKNOWLEDGMENT

Thanks are owed to the outstanding attorneys at U.S. Strategic Command, U.S. Cyber Command, and the U.S. Joint Staff who the author has been privileged to work with and for over the past four years. And a debt is forever owed to MJF and GJD for helping carve out time to read, write and edit and for encouraging critical thinking.

[94] *See supra* notes 59-60, and accompanying text.

[95] Pwned is a common hacker slang term for when one system is "owned" i.e. controlled by or defeated by, another system. It likely came about from a typo due to the proximity of the "p" and "o" keys on a qwerty keyboard. *See* PWN, Wikipedia, http://en.wikipedia.org/wiki/Pwn (last visited Jan. 4, 2015).

[96] *See supra*, note 89, and accompanying text.

[97] *See supra* note 90, and accompanying text.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace

Paul A. Walker
Commander
U.S. Navy, Judge Advocate
General's Corps (Retired)
Washington, DC
Paul.walker@1987.usna.com

Abstract: States are rapidly approaching an international law crossroads in cyberspace. While many States, led by the United States, take the view that existing international law, including the law of armed conflict, is sufficient to cover cyberspace ("law of the horse"), such a view is being overtaken by reality. The Sony hack allegedly by North Korea is only the latest, and most blatant, in the long history of State activity in cyberspace. The current architecture of cyberspace makes it very attractive for States to pursue their national interests via this domain in a manner that is easily denied. With such a state of affairs persisting into the foreseeable future, it is very likely that international law will soon be sidelined or ignored by States as they seek to respond to cyber activity undertaken by other States ("law of the submarine"). With most, if not all, State-sponsored cyber activity not rising to the level of a use of force, countermeasures are one of the most viable international law tools for States to respond to State-sponsored cyber activity. Countermeasures, however, is the international law concept most at risk of being ignored by States. The customary international law of countermeasures imposes many conditions and limitations on their use, conditions and limitations that States will be inclined to ignore because they can under cyberspace's current architecture. Fortunately, the customary international law of countermeasures remains fluid enough that it can be sufficiently adapted to accommodate State behavior in cyberspace while still accounting for the international law interests underlying countermeasures.

Keywords: *international law, countermeasures, cyber activity, State action*

1. INTRODUCTION

"We will respond proportionally [to North Korea's hack of Sony], and we'll respond in a place and time and manner that we choose." – President Obama, December 19, 2014[1]

North Korea's alleged hack of Sony Pictures Entertainment is only the most recent – and most blatant – example of a State using cyberspace to pursue its national interests. Nation-States are suspected of actions against other nation-States as far back as the "Moonlight Maze" series of intrusions in 1999.[2] But beginning with Estonia in 2007,[3] alleged State actions have become increasingly visible. In addition, from Estonia (2007) to Georgia (2008)[4] to Stuxnet (2010-11)[5] to Saudi ARAMCO (2012)[6] to denials of service against U.S. banks (2012-13)[7] to Sony (2014)[8], one can trace a nearly linear line of increasingly disruptive, and potentially destructive, activity that is "attributed" to nation-States. Yet, no State has admitted undertaking these actions and no entity has provided absolute proof that a State was behind any of these malicious cyber actions. Taken alone, none of these events rises to the level of the cyber "pearl harbor" that is so often trumpeted.[9] Unfortunately, although international law is well-equipped to deal with a cyber "pearl harbor," it is not as well-equipped to deal with the current situation of unacknowledged and unattributed State actions not amounting to a use of force or an armed attack in cyberspace. This paper proposes modifications to the customary international law of countermeasures that are necessary to redress that deficiency in international law.

Modifications are necessary because the current architecture of cyberspace makes it very attractive for States to ignore international law. The internet's architecture makes it easy for States to achieve national security objectives through the interconnectedness of cyberspace, while maintaining the ability to deny their actions. The concept of deniability extends well beyond the usual problems of attribution and is particularly useful for States. Even when a State

[1] Remarks by the President in Year-End Press Conference, The White House, Dec. 19, 2014, available at http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

[2] Bob Drogin, *Russians Seem To Be Hacking Into Pentagon*, SFGATE, Oct. 7, 1999, at http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.

[3] *See, e.g.*, Eneken Tikk, Kadri Kaska and Liis Vihul, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 18-24 (2010) (describing the distributed denial of service actions against Estonia and their effects), available at https://ccdcoe.org/sites/default/files/multimedia/pdf/legalconsiderations_0.pdf.

[4] *See, e.g.*, John Bumgarner & Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, A US-CCU Special Report, 6 (Aug. 2009).

[5] *See generally* Kim Zetter, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014); *see also* David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, Jun. 1, 2012 at A1 (citing anonymous sources attributing Stuxnet to the U.S. and Israel as part of a program named "Olympic Games").

[6] *See, e.g.*, Byron Acohido, *Why the Shamoon Virus Looms as a Destructive Threat*, USA TODAY, May 16, 2013, available at http://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/.

[7] Ellen Nakashima, *U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks*, WASH. POST, Apr. 11, 2014, available at http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

[8] *See, e.g.*, Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[9] *See, e.g.*, Leon E. Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, Oct. 11, 2013 ("The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."), at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

makes a prompt, public and affirmative attribution of cyberspace activity to another State[10], it is difficult to demonstrate and ensure the accuracy of that attribution[11] and the offending State still has the ability to deny responsibility. Because of the interconnected, global nature of the internet, States are able to achieve effects remotely, without placing personnel or other assets at physical risk.[12] As a result, States of all sizes are finding it easier than ever to accomplish national security objectives, whether disrupting an adversary's propaganda efforts,[13] sending active and visible messages of their own,[14] conducting aggressive intelligence collection[15] or conducting support to military operations[16] and sabotage.[17]

This paper begins with a brief overview of the positions that the leading States have taken with regard to the applicability of international law in cyberspace. Although Russia and the United States have long differed over the need for a treaty for cyberspace, the prevailing view, as articulated by the United States, is that existing international law norms are sufficient for addressing State activity in cyberspace. Such a position, though, is at odds with the apparent behaviour of States in cyberspace, where national interests are pursued without fear of responsibility or accountability. The next section examines a similar historical example where international law did not keep pace with technological developments and State practice, leading to the declaration of unrestricted submarine warfare by the U.S. immediately upon entry into World War II, an action not consistent with then-prevailing international law. Next, the difficulties of applying the customary international law of countermeasures in cyberspace are examined. The final section of the paper proposes modifications to the customary international law of countermeasures designed to accommodate State behaviour while still accounting for the international law interests underlying countermeasures.

2. "LAW OF THE HORSE" OR WHAT STATES SAY

In 1996, Judge Frank Easterbrook delivered a seminal lecture at the University of Chicago ostensibly about "Property in Cyberspace."[18] Judge Easterbrook took the opportunity to

[10] The leading example is the U.S. attribution of the Sony hack to North Korea. *See* Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[11] See *infra* note 60-61, and accompanying text.

[12] *See, e.g.*, Elizabeth Flock, *Operation Cupcake: MI6 Replaces al-Qaeda Bomb-Making Instructions with Cupcake Recipes*, WASH. POST, Jun. 3, 2011 (describing efforts by the United Kingdom to disrupt the publication of al Qaeda in the Arabian Peninsula's *Inspire* magazine), at http://www.washingtonpost.com/blogs/worldviews/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html.

[13] *See, e.g.*, Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, WASH. POST, Mar. 19, 2010 at A1.

[14] *See, e.g.*, Acohido, *supra* note 6 (describing the Shamoon virus as an Iranian response to a wiper virus used against Iran's oil industry); Ben Elgin and Michael Riley, *Now at the Sands Casino: An Iranian Hacker in Every Server*, BloombergBusiness, Dec. 11, 2014 (describing an alleged Iranian action against Sands Casino because of anti-Iranian statement made by the casino's owner), available at http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

[15] *See, e.g.*, Michael Riley, *How Russian Hackers Stole the NASDAQ*, BUSINESS WEEK, Jul. 17, 2014 ("By mid-2011, investigators began to conclude that the Russians weren't trying to sabotage Nasdaq. They wanted to clone it, either to incorporate its technology directly into their exchange or as a model to learn from.").

[16] *See* Bumgarner & Borg, *supra* note 4, at 6.

[17] *See generally* Zetter, *supra* note 5; *see also* Sanger, *supra* note 5, at A1 (citing anonymous sources attributing Stuxnet to the U.S. and Israel as part of a program named "Olympic Games").

[18] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.

question the very premise not only of his assigned topic, but the underlying premise of the conference that there was a need to adapt law for cyberspace.[19] Instead, Judge Easterbrook advocated for the application of existing legal principles to cyberspace.[20] He pointed to the fact that law schools do not teach a "law of the horse," as an analogy, arguing that "the best way to learn the law applicable to specialized endeavors is to study general rules" rather than trying to pull the strands of various areas of law (i.e., torts and contracts) into a "Law of the Horse" course.[21] Importantly, Judge Easterbrook did recognize that existing law is often flawed, even in the way that it applies outside of cyberspace.[22] Accordingly, he suggested that cyberspace could act as a type of catalyst to ensure the refinement of existing law through the implementation of sound principles that can be applied both outside and inside cyberspace.[23]

Despite the strength of his logic, Judge Easterbrook's position was strongly challenged by internet advocates, such as Lawrence Lessig.[24] Today, there are a number of legal texts dealing with "Cyberlaw" and many law schools have a similarly-titled course. Today, Judge Easterbrook's position finds much more support in the application of existing international law principles to cyberspace. The leading proponent of this view is the United States.

In 2011, the U.S. issued its *International Strategy for Cybersecurity*,[25] one of the first countries to do so. With respect to international law, the U.S. strategy stated there was no need to reinvent international law and that international norms are not "obsolete."[26] Although acknowledging the need for "additional work" to clarify how these norms apply in cyberspace, "[l]ong-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace."[27] The U.S. position was further clarified publicly by Harold Koh, then the U.S. State Department's Legal Adviser. In a speech to the U.S. Cyber Command legal conference in September, 2012, Koh affirmed that international law does apply in cyberspace.[28] But he also went a step further. Alluding to Russian proposals for a new treaty to apply to the "cutting edge issues presented by the internet," Koh decisively rejected the need for new international law based on the uniqueness of cyberspace: "Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law do apply in cyberspace."[29] In short, the "law of the horse" is rejected; what we have is good enough as long as we apply it properly.

Unfortunately, agreement on how international norms apply in cyberspace has been slow to develop. It was only in 2013 that the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, a group that included Russia and China in addition to the U.S., were able

[19] *Id*.

[20] *Id*. at 208.

[21] *Id*. at 207.

[22] *Id*. at 209.

[23] *Id*.

[24] *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, HARV. L. REV. 501 (1999).

[25] White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011.

[26] *Id*. at 9.

[27] *Id*.

[28] Harold Hongju Koh, International Law in Cyberspace: Remarks to the USCYBERCOM Inter-Agency Legal Conference, Sept. 18, 2012, available at http://www.State.gov/s/l/releases/remarks/197924.htm.

[29] *Id*.

to report agreement that international law and the UN Charter were applicable to cyberspace.[30] The 2010 report from the same group was unable to reach agreement on that point. Even with the publication of the 2013 report, there is still disagreement over the application of international law in cyberspace. Russia is still interested in implementing this concept via a new treaty. China, meanwhile, remains distrustful of western efforts to apply international law to cyberspace, denigrating efforts such as the Tallinn Manual for providing too permissive an atmosphere in cyberspace for the actions of western countries such as the United States.[31]

Despite agreement that international law applies in cyberspace, as discussed in the introduction there is growing evidence that States are behaving as if there are few, if any, restraints in the conduct of cyberspace activities.[32]

3. "LAW OF THE SUBMARINE" OR THE FUTURE OF STATE BEHAVIOR IN CYBERSPACE

States have ample incentive to pursue their national security interests via cyberspace in a manner that is not transparent. Some commentators correctly point out that the lack of transparency inhibits the development of international norms and the advancement of international law. Eichensehr, for instance, criticizes the fact that the U.S.'s 2011 *International Strategy for Cyberspace* does not adequately state what precise norms the United States is seeking.[33] As a result, the U.S. "is missing the opportunities to foster development of norms."[34] Jack Goldsmith also warns of the dangers of not being forthcoming with information: "[the FBI's] hesitation in the face of credible questions about its very thin public evidence will exacerbate the demand for publicly verifiable attribution before countermeasures (or other responses) are deemed legitimate."[35] But the failure to develop international norms of behaviour and advance the development of international is not the greatest danger to the international system of States' demonstrated behaviour in cyberspace. The greater danger is that international law will be ignored altogether, a situation that is not without precedent.

Within hours of the attack on Pearl Harbor, the U.S. Navy Chief of Naval Operations (CNO) knowingly ordered the Navy to violate international law by directing the use of unrestricted

[30] United Nations, REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, Jul. 30, 2013, at 2, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[31] Adam Segal, NATO's *Take on Cyberspace Law Ruffles China's Feathers*, DEFENSE ONE, Oct. 29, 2014 (summarizing an article in the People's Liberation Army Daily critical of the Tallinn Manual "as an effort to manipulate cyberspace using law" and as a way for the U.S. to maintain its dominance).

[32] See *supra* notes 10-17, and accompanying text.

[33] Kristen Eichensehr, *The US Needs a New International Strategy for Cyberspace*, JUST SECURITY, Nov. 24, 2014, at http://justsecurity.org/17729/time-u-s-international-strategy-cyberspace/.

[34] *Id*.

[35] Jack Goldsmith, *The Consequences of Credible Doubt About the USG Attribution in the Sony Hack*, LAWFARE, Dec. 30, 2014, at http://www.lawfareblog.com/2014/12/the-consequences-of-credible-doubt-about-the-usg-attribution-in-the-sony-hack/.

submarine warfare against Japan.[36] International law then (and now) required submarines to remove a merchant vessel's crew to a place of safety before sinking the merchant vessel and a lifeboat on the open sea did not suffice as a place of safety.[37] These "cruiser rules," applying as they did to any merchant vessel regardless of whether it was flagged to a belligerent or a neutral,[38] were untenable for submarines, whose great advantage lay in the stealth and surprise afforded by hiding under the sea and who are very vulnerable on the surface.[39] Nor did submarines have sufficient manning to provide prize crews that could sail the merchant vessel to a friendly port. Faced with the irreconcilable difference between the dictates of international law and effective military strategy, Navy leaders chose to ignore international law.

Confronted with increasingly disruptive and frequent State activities in cyberspace, States today are confronting a similar dilemma. With all cyberspace activity to-date falling below the level of an armed attack[40] that would provide the ability to use force in self-defense, countermeasures are one of the most viable options for States to use in responding to current levels of State cyber activity. Yet, the current legal framework for countermeasures is not compatible with State's demonstrated behaviour in cyberspace.

4. THE COUNTERMEASURE DIFFICULTY

Countermeasures are State actions that would normally be considered a violation of international law, but become justified by the fact that they are undertaken in response to another State's internationally wrongful act.[41] It is generally understood that a proper countermeasure should not amount to a use of force and must not violate any other peremptory norm of international law.[42] Beyond network defense actions and multilateral efforts, there are a variety of active cyberspace-based responses that could be used as a countermeasure. One such countermeasure

[36] Joel Ira Holwitt, "EXECUTE AGAINST JAPAN:" THE U.S. DECISION TO CONDUCT UNRESTRICTED SUBMARINE WARFARE 14 (2008). Although the CNO's order was issued roughly four-and-a-half hours after the attack on Pearl Harbor, his was not the first U.S. Navy order to do so. The Commander of the Asiatic Fleet, Admiral Hart, ordered his air and submarine units to carry out unrestricted warfare three hours earlier, but Admiral Hart knew that the CNO was going to issue the same order on the outbreak of hostilities. *Id*. at 156. The CNO's decision came after "a year of debate and consideration by the U.S. naval leadership." *Id*. at 15.

[37] *Id*. at 58-59 (describing how only five years earlier the United States had signed the London Submarine Protocol, which re-affirmed Article 22 of the London Naval Treaty of 1930 requiring submarines to adhere to "cruiser rules" with respect to merchants).

[38] *Id*.

[39] *Id*. Holwitt points to an early article by a young Lieutenant Hyman Rickover, later the "father of the nuclear Navy," that succinctly makes the point: "The conclusion is inevitable that, except in rare circumstances, it is impossible for the submarine to carry on commerce warfare in accordance with international law as it stands today. Consequently, states must either renounce this weapon as a commerce destroyer or undertake a revision of the laws governing naval warfare, taking into account the changed conditions of modern war. . ." *Id*. at 61, quoting from H. G. Rickover, *International Law and the Submarine*, 61 PROCEEDINGS 1219 (Sept. 1935).

[40] Michael N. Schmitt, ed., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 57 (2013) [hereinafter TALLINN MANUAL] ("No international cyber incidents have, as of 2012, been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack."). There have been not been any that met this criteria in the years since, either.

[41] Draft Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission, Art. 22 (2001) [hereinafter *Draft Articles*] ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State…").

[42] *Id*. at 131, Art. 50.

is designed to get the offending activity to stop, or "cease and desist."[43] For example, an action that causes an offending web browser to close without affecting any other part of the computer.[44] Likewise, suborning a botnet's command and control channel and telling the botnet to shut itself off or to delete itself,[45] or to direct its activity at a sinkhole IP address[46] would be other examples of non-cooperative "cease and desist." A more active approach is what has come to be known as "hack back," which involves accessing the offending computer(s) for the purpose of retrieving stolen data by deleting it from the possession of the offender, deleting malicious programs, or corrupting, in a reversible manner, the computer(s) that is the origin of the offending cyber activity.[47] An active response not involving a "hack back" might involve the use of a distributed denial of service (DDoS) against an IP address or server that is the origin of malicious activity, or is controlling malicious activity, in order to prevent the activity from affecting the defender's system. By any reasonable measure, these kinds of actions are not forcible countermeasures. They do not result in deaths, injuries, or significant physical destruction,[48] nor do they reach the levels of severity, invasiveness, and measurability of effects, among other factors, that may lead to a use of force conclusion.[49]

The purpose of using a countermeasure is to effect a return to the *status quo ante*, that is, to get the offending State to resume its obligations under international law.[50] As such, the countermeasure(s) that a State undertakes should generally be temporary and reversible, so as not to create a permanent violation of international law.[51] This is a requirement that is easily met with cyberspace operations and is a key reason why cyberspace activity should be, and is, very attractive as a countermeasure. For instance, Heather Harrison Denniss notes that in 1998 the U.S. Department of Defense responded to "Floodnet" attacks against the Defense Department website with a program that closed the internet browser on the computers sending the "Floodnet" applet.[52] By generating this minimal result on all such computers, wherever located, the malicious activity against the website stopped. Although the action was taken against a non-state actor, Denniss views this outcome as an appropriate proportionate countermeasure.[53] While the temporary and reversible requirement for cyber countermeasures may not pose a difficulty, the same cannot be said of other limitations on countermeasures.

[43] William A. Owen, Kenneth W. Dam, Herb Lin, eds., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 149 (2009) ("Non-cooperative 'cease and desist'" is "the use of tools to disable harmful services on the attacker's system without affecting other system services.").

[44] Heather Harrison Denniss, CYBER WARFARE AND THE LAWS OF WAR 108 (2012), citing Brian Friel, DoD Launches Internet Counterattack, GOV'T EXECUTIVE (Sept. 18, 1998) (describing DoD action against malicious cyber activity in the late-1990s).

[45] Paul Bacher, Thorsten Holz, Markus Kotter, Georg Wicherski, Know Your Enemy: Tracking Botnets (describing efforts to infiltrate BOTNETs using command and control channels), at https://www.honeynet.org/book/export/html/50.

[46] Federal Bureau of Investigation, GameOver Zeus Botnet Disrupted (Jun. 2, 2014) (describing the use of " measures to sever communications between the infected computers, re-directing these computers away from criminal servers to substitute servers under the government's control").

[47] Owen, Dam, & Lin, *supra* note 43, at 149.

[48] Koh, *supra* note 28, at 3 (describing the U.S. position that cyber activity causing deaths, injuries or significant physical destruction is an illegal use of force).

[49] TALLINN MANUAL, *supra* note 40, at 48-51 (discussing an approach designed "to assess the likelihood that States will characterize a cyber operation as a use of force), citing Michael N. Schmitt, *Computer Networks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999).

[50] *Draft Articles, supra* note 41, at 129, Art. 49(1).

[51] *Id*., Art. 49(3).

[52] Denniss, *supra* note 44, at 108.

[53] *Id*.

The customary international law of countermeasures imposes a number of limitations and conditions on the use of countermeasures. As an initial matter, countermeasures may only be taken "against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations" under international law.[54] In order to take countermeasures, therefore, a State is required to identify the State responsible for the internationally wrongful act. Once thought difficult, attribution of State action in cyberspace is becoming quite common. Anti-virus companies are at the forefront of these efforts, with the latest salvo a Kaspersky report identifying a group it calls the "Equation Group," which Kaspersky equates to the U.S.'s National Security Agency.[55] But States are beginning to publicly attribute internationally wrongful acts in cyberspace to other States, as well. Most prominently, in December, 2014, the United States made a prompt, public, affirmative statement[56] that North Korea was responsible for the hack of Sony Pictures Entertainment and the subsequent release of large quantities of company proprietary data and employee emails. Although North Korea has repeatedly and continuously denied this claim by the United States, the Federal Bureau of Investigation (FBI) claim is based on methodologies similar to those used by multiple anti-virus vendors in forensic reports claiming State sponsorship of cyber activity.

For instance, the FBI claimed that the command and control infrastructure used in the Sony hack overlapped "significant[ly]" with that observed in previous North Korean actions, including the use of internet protocol (IP) addresses "associated with known North Korean infrastructure" communicating with other IP addresses that were "hardcoded into the data deletion malware" used against Sony.[57] Mandiant and Kaspersky both made similar infrastructure claims in their reports attributing "APT 1" ("APT" stands for "advanced persistent threat") and Equation Group as the Chinese People's Liberation Army Unit 61398 and the U.S.'s National Security Agency, respectively.[58] Likewise, Mandiant, Kaspersky and FireEye (Mandiant's successor) also rely heavily on repeated uses of the same or similar software, often from software "families," which is not that different from the FBI's assertion that the data deletion malware was similar to "other malware that the FBI knows North Korean actors previously developed."[59] Despite these similarities to commonly used forensic methodologies, the U.S. attribution to

[54] *Draft Articles, supra* note 41, Art. 49(1).

[55] Dan Goodin, How "Omnipotent" Hackers Tied to NSA Hid for 14 Years—and Were Found at Last, Ars Technica (Feb 16, 2015), at http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.

[56] Federal Bureau of Investigation, Update of Sony Investigation, FBI National Press Office, Dec. 19, 2014, at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[57] *Id*.

[58] APT1: Exposing One of China's Cyberespionage Units, Mandiant 39-40 (describing infrastructure, including a large number of IP addresses and domain names, used by APT1 as hop points in their operations, with the activity leading back to four networks in the Shanghai area where Unit 61398 is based).

[59] *Id*.

North Korea was not universally accepted by the information security community.[60] This may be due to the rapidity of the attribution claim, as well as the fact that it did not come in the type of lengthy and detailed report the industry is used to digesting. The failure to provide additional details undoubtedly accounts for a substantial portion of the negative reaction,[61] bolstered by the FBI's intimation that it relied on intelligence community sources not available to the information security community. Ultimately, though, it is up to the State to determine whether an internationally wrongful act has occurred and which State is responsible for that act, understanding that it may be held responsible for countermeasures taken erroneously.[62]

Once a State determines the State behind an internationally wrongful act, countermeasures may only be taken against that State. As the commentary to this portion of the Draft Articles on State Responsibility (Draft Articles) puts it, "Countermeasures may not be directed against States other than the responsible State."[63] Such a stricture presents particular difficulties in cyberspace when the offending activity may be initiated by a single State, but use infrastructure and equipment located in third States to carry out the cyber activity. As an example, the Iranian DDoS against U.S. bank websites used a network of compromised, linked computers (called a "botnet") to execute the DDoS action.[64] Most, if not all, of these computers were located in countries around the globe, not Iran. The owners of the compromised equipment, much less the State where geographically situated, had no idea they were compromised or the purpose for which they were used. Yet, to take action against these nodes of the botnet, even if it is the easiest, most temporary and reversible method, would seem to be precluded by the customary international law of countermeasures. The U.S. seems to agree with this approach, as when confronted with this situation, rather than acting unilaterally, it reached out to 120 nations in an effort to get those countries to directly address the offending behaviour.[65] Unfortunately, this effort did not lead to a significant diminution of the strength of the DDoS activity, which only ceased with a change in the Iranian domestic political situation.[66]

[60] In addition to criticism of the FBI for relying on its own previous (unpublished) attribution, researchers also pointed out that the wiper malware used by North Korea was related to other such malware, including the Shamoon malware used against the Saudi ARAMCO oil company and widely attributed to Iran. Marc Rogers, Why I *still* Don't Think It's Likely that North Korea Hacked Sony, Marc's Security Ramblings, Dec. 21, 2014 (comparing Destover, the wiper malware used against Sony, to the Shamoon wiper malware used in Saudi Arabia and the Dark Seoul wiper malware used against South Korea), at http://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony/. *See also* Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED, Dec. 3, 2014 (describing the use of the same commercially-available driver to do the wiping of data in Sony, Shamoon and Dark Seoul, which indicates not necessarily the same group, but easily copied techniques), at http://www.wired.com/2014/12/sony-hack-what-we-know/. Other criticism focused on how easily the IP addresses that were "associated" with North Korea could be spoofed or hacked. Kim Zetter, *Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy*, WIRED, Jan. 8, 2015, at http://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy/.

[61] For instance, the FBI had a three-hour meeting with one cybersecurity firm that presented evidence the Sony hack was the work of "disgruntled" former Sony employees. *See* Tal Kopan, *U.S.: No Alternate Leads in Sony Hack*, POLITICO, Dec. 29, 2014 (describing the meeting between cyber intelligence company Norse and FBI officials), at http://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.html.

[62] *Draft Articles*, supra note 41, at 130 ("A State which resorts to countermeasures based on its unilateral assessment of the situation does so at its own risk and may incur responsibility for its own wrongful conduct in the event of an incorrect assessment.").

[63] *Id*. at 130.

[64] Nakashima, *supra* note 7.

[65] *Id*.

[66] *Id*.

In addition to being taken against the offending State, countermeasures may only be undertaken while the internationally wrongful act is ongoing.[67] Once the internationally wrongful act has ceased, the countermeasure may not be initiated or, if already begun, must terminate.[68] This poses some difficulty in responding to cyberspace operations because often the internationally wrongful act may be a series of discreet acts or a single discreet event that, even when completed, may have ongoing repercussions. For instance, although the Iranian DDoS activity did not occur on a continual basis, it did periodically repeat itself for an extended period of time. The question then arises as to whether countermeasures may only be taken during an active DDoS event or could also occur in a lull so as to prevent another incident. Also problematic is the example of the Sony hack, where arguably North Korea's alleged internationally wrongful act ended up as a singular, completed event once the hackers announced their presence and absconded with Sony's proprietary information.

Given State behaviour in cyberspace as described in the introduction, particularly the demonstrated desire for deniability, the requirement to call upon the responsible State to fulfil its international law obligations is also problematic.[69] The purpose of this requirement is to give the offending State "notice of a claim and some opportunity to present a response" due to the "serious consequences of countermeasures."[70] The Commentary to the Draft Articles contemplates a period of "extensive and detailed" negotiations before the point of countermeasures is reached, with the notice requirement often inherent in these negotiations.[71] However, cyberspace activity will not generally lead to negotiations, given the deniability outcome. In fact, even when called upon to cease cyberspace activity, States such as China continue to deny their responsibility, even in the face of numerous well-sourced reports and indictments. Once States decide to undertake non-forcible countermeasures, there will usually be a need for much quicker action in the cyberspace domain. States may be unwilling to attribute internationally wrongful acts either publicly or directly to the State for fear of losing the ability to take effective countermeasures.

The second notice requirement, to inform the "responsible State of any decision to take countermeasures and offer to negotiate with that State"[72] is actually much less problematic because there is an "out" clause.[73] Specifically, this second notice provision is not required when the aggrieved State needs to take "urgent" countermeasures to preserve its rights, including its right to take countermeasures.[74] The out clause is provided in the event that notice to the offending State would allow it to take steps to "immunize" itself from the countermeasures.[75] In the case of cyber countermeasures, use of this exception will be a given in virtually every case in order to ensure chosen countermeasures remain effective.

[67] *Draft Articles, supra* note 41, Art. 52(3)(a).
[68] *Id*. at 136.
[69] *Id*., Art. 52(1)(a).
[70] *Id*. at 136.
[71] *Id*.
[72] *Id*., Art. 52(1)(b).
[73] *Id*., Art. 52(3).
[74] *Id*. at 136.
[75] *Id*.

5. COUNTERMEASURES FOR THE DIGITAL AGE

There are three adjustments necessary to keep the customary international law of countermeasures relevant in the digital age. First, and most easily accomplished, the exception to the requirement to notify an offending State of the decision to take countermeasures should also apply to the requirement to call on the offending State to stop the international wrongful act. Instead, this requirement should be shifted to prompt notification *after* taking countermeasures. This change is necessitated by the need for States to retain the ability to take effective countermeasures. As seen with the Sony hack, even when one State implicates another in cyber activity that probably constitutes an internationally wrongful act, the nature of cyberspace is such that the accused State can plausibly continue to deny responsibility. Permitting States to wait until after-the-fact of countermeasures to call on a state to comply with its international obligations will encourage States to treat any response action they take not as punitive, but as a proper countermeasure, one which retains its effectiveness. Once the offending State is asked to resume its obligations under international law and learns of the fact of countermeasures, it then still has a full panoply of actions available to it under international law, including seeking redress for the countermeasure in an appropriate international forum. Of course, the preferred course of action by the offending State is to cease the original internationally wrongful act.

The second needed adjustment is clarification of when an internationally wrongful act in cyberspace ceases or is no longer ongoing. The focus of this limitation should not be on any single, discrete activity, but should focus on the broader failure of a State to live up to its obligations under international law on a continuing basis. As a result, countermeasures may then be available to a State during periods of inactivity, when there is a pattern of active and passive behaviour, or even after a discrete event when the effect of the discrete event is to support an ongoing wrong that is different in scope. For instance, in the case of the alleged Iranian DDoS activity against U.S. banks, once an active-inactive pattern is established, countermeasures could be taken during periods of inactivity in order to prevent further activity. In the case of the Sony hack, a case could be made that there is an ongoing violation of the non-intervention principle in the way that the alleged North Korean hackers are making use of the information to continue to harm Sony or other U.S. economic interests. In that instance, it may be appropriate to take a countermeasure designed to recover the stolen data by making it no longer useable by the hacker or to prevent its continued use in harming U.S. economic interests.

Finally, for countermeasures to remain a viable legal concept in cyberspace, they will need to remain effective as a practical matter, as well. To be effective, countermeasures in cyberspace will have to occur in the territory of third-party States. Note well, though, that while effective cyber countermeasures may need to occur *in* the territory of a third-party State, those countermeasures are not directed *against* that third-party State. Such countermeasures would remain directed against the cyber activities of the original, offending State, which itself is potentially committing an internationally wrongful act against the third-party State in the course of carrying out the activity against the receiving State. It is worth remembering, in that vein, that the cyber activity used to compromise equipment in that third-party State is usually occurring unbeknownst to the State or the owner of the equipment and thus neither has any rational interest in the continued operation of the malware or exploit used to carry out the internationally wrongful act. Taking limited action to stop a botnet operation by using its own commands against it, including the possibility of telling it to delete itself, would not unduly impinge on core interests of the third-party State. Such action could easily be viewed as the type of "incidental" effects that typically occur in third States when one State takes economic countermeasures against another State. The Draft Articles use the suspension of a trade agreement as an example where one or more companies in third States "lose business or even go bankrupt" as a result of suspended trade with the responsible State. It is fair to say that a bankrupt company has a much greater impact on the third State's economy than simply deleting unknown and unwanted software or other minimal measures causing only temporary changes to the equipment, such as soft reboots.

6. CONCLUSION

State behaviour in cyberspace is going to look much like it has in the present and the past, including when using cyber measures to conduct countermeasures (or retaliation). States that are leaders in the area of cyberspace, such as the United States, are missing the opportunity to develop international norms. Moreover, there is great risk that the customary international law of countermeasures will be ignored altogether because it is too cumbersome to apply to cyberspace operations. Allowing States to take non-forcible cyber countermeasures against the effects of—or a pattern of—internationally wrongful acts, even if the countermeasure needs to occur in the cyber infrastructure of a third State followed by after-the-fact notification to those States, will keep the customary international law of countermeasures relevant for the digital age. These adjustments will also encourage more transparency by States, transparency that is urgently needed to advance legal discussion not only in the area of countermeasures, but all areas of international law impacted by State behaviour in cyberspace.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?

Uchenna Jerome Orji
African Centre for Cyber Law and Cybercrime
Prevention (ACCP)
Kampala, Uganda
jeromuch@yahoo.com

Abstract: Within the past decade, Africa has witnessed a phenomenal growth in Internet penetration and the use of Information Communications Technologies (ICTs). However, the spread of ICTs and Internet penetration has also raised concerns about cyber security at regional and sub-regional governance forums. This has led African intergovernmental organizations to develop legal frameworks for cyber security. At the sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Directive on Cybercrime, while the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have adopted model laws. At the regional level, the African Union (AU) has adopted a Convention on Cyber Security and Personal Data Protection. This paper seeks to examine these legal instruments with a view to determining whether they provide adequate frameworks for mutual assistance and international cooperation on cyber security and cyber crime control.

The paper will argue that the AU Convention on Cyber Security and Personal Data Protection does not provide an adequate framework for mutual assistance and international cooperation amongst African States and that this state of affairs may limit and fragment international cooperation and mutual assistance along sub-regional lines or bilateral arrangements. It will recommend the development of international cooperation and mutual assistance mechanisms within the framework of the AU and also make a case for the establishment of a regional Computer Emergency Response Team to enhance cooperation as well as the coordination of responses to cyber security incidents.

Keywords: *African Union, Computer Emergency Response Teams, dual criminality, Mutual Legal Assistance*

1. INTRODUCTION

Since the beginning of the 21st century, Africa has continued to witness a phenomenal growth in Internet penetration and the use of ICTs. Statistical data indicates that Internet users in Africa grew from 4,514,400 million people in 2000 to 297,885,898 million people in June 2014.[1] This phenomenal growth which is still in progress[2], has been linked to factors such as the liberalization of the telecommunications market in African States, the widespread availability of mobile technologies, and the increasing availability of broadband systems.[3] However, the spread of ICTs and Internet penetration in African states has also raised concerns about cyber security at regional and sub-regional governance forums. Consequently, some African intergovernmental organizations have developed legal frameworks for cyber security. At the sub-regional level, the Economic Community of West African States (ECOWAS) adopted a Directive on Fighting Cybercrime in August 2011, while the Common Market for Eastern and Southern Africa (COMESA) adopted a Model Cybercrime Law in October 2011. The Southern African Development Community (SADC) also adopted a Model Law on Computer Crime and Cybercrime in March 2012. At the regional level, the African Union (AU) has adopted the AU Convention on Cyber Security and Personal Data Protection in June 2014. Already, some African States have established national legal and policy frameworks for cyber security, while many others are developing such frameworks. However, a discussion of national cyber security initiatives is beyond the scope of this paper.[4] This paper seeks to examine Africa's regional and sub-regional legal frameworks on cyber security with a view to determining whether they can provide a basis for mutual assistance and effective international cooperation in the control of cyber crime and promotion of cyber security.

The paper will argue that the AU Convention on Cyber Security and Personal Data Protection does not provide an adequate legal framework for mutual assistance and international cooperation amongst African States and that this state of affairs may limit and fragment international cooperation and mutual assistance along sub-regional lines or bilateral arrangements. It will recommend the development of international cooperation and mutual legal assistance mechanisms within the framework of the AU and also make a case for the establishment of a regional Computer Emergency Response Team to enhance cooperation in the coordination of responses to cyber security incidents.

The paper is divided into five sections. The first section which includes this introduction will provide an overview of the concepts of cyber security, and international cooperation and also present a general background on Africa. The second section will critically examine the AU Convention on Cyber Security and Personal Data Protection to determine whether it provides an adequate framework for mutual assistance and international cooperation amongst African States, while also comparing the Convention with the Council of Europe Convention on Cybercrime. The third section will examine sub-regional cyber security frameworks such as the ECOWAS Directive on Fighting Cybercrime, the COMESA Model Cybercrime Bill and the

[1] *See* Miniwatts Marketing Group, "Internet Usage and Population Statistics for Africa", (June 30, 2014), available at <http://www.internetworldstats.com/stats1.htm>.

[2] *See* ITU Telecommunication Development Bureau, *The World in 2014 –ICT Facts And Figures*, available at <http://www.itu.int/en/ITU-D/Statistics/Documents/ICTFactsFigures2014-e.pdf>.

[3] *See* GSMA, *The Mobile Economy Report 2013* (A.T. Kearney: London, United Kingdom, 2013) p.16.

[4] For a discussion of cyber security initiatives in African States, *see* Uchenna Jerome Orji, *Cybersecurity Law and Regulation* (Wolf Legal Publishers: Netherlands, 2012) pp.401-485.

SADC Model Law on Computer Crime and Cybercrime to determine whether they also provide a framework for mutual assistance and international cooperation amongst Member States. The fourth section will propose both legal and other governance measures to strengthen mutual assistance and international cooperation on cyber security amongst African States, while the fifth section concludes the paper.

1.2. An Overview of Basic Concepts

1) Cyber Security

Cyber security is an information age terminology that was derived by merging the prefix – "cyber" with the concept of "security". The term is defined as "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assets".[5] Cyber security governance measures include technical, organizational, policy, and legal aspects.[6] The technical aspects of cyber security governance deal with the development and implementation of technical protection measures for computer systems and network infrastructure, while the organizational aspects deal with the development of institutional capacities to promote cyber security such as the establishment of law enforcement organizations as well as the development of institutional capacities such as the establishment of Computer Emergency Response Teams (CERTs) to provide critical services such as prevention and early warning, detection and management of cyber security incidents.

On the other hand, the legal aspects of cyber security governance deal with legal measures that aim to promote cyber security. Legal measures are usually considered as probably the most relevant aspect of cyber crime control.[7] Such measures include the establishment of laws prohibiting acts that violate the security or integrity or availability of computer data and systems or networks and attacks against critical information infrastructure. It also includes measures to facilitate cross-border cooperation on cyber security with respect to the prevention, investigation and prosecution of prohibited acts. The scope of cyber security laws may also extend to the criminalization of acts that do not affect the security of computers or data or networked information infrastructure such as online child pornography or online xenophobia[8]. Malicious acts that are prohibited by cyber security laws are commonly referred to as "cyber crime" or "computer crime". These terms are often used interchangeably to refer to instances where computer technologies are the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. However, there is no universally accepted legal definition of cyber crime or computer crime[9] and cyber security laws generally tend to avoid such explicit definitions.[10]

[5] *See* ITU High Level Experts Group [HLEG] *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report* (ITU: Geneva, 2008), p.27. See Uchenna Jerome Orji, Cybersecurity Law and Regulation, at pp.10-16.

[6] *See* Uchenna Jerome Orji, *Id.*, at pp.17-42.

[7] *See* Gercke Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU: Geneva, 2009) p.84.

[8] However, some countries regard the criminalization of the online dissemination of xenophobic materials as an impediment to free speech. *See* Kristin Archick "Cybercrime: The Council of Europe Convention", *CRS Report for Congress*, (September 28, 2006) p.3.

[9] *See* Uchenna Jerome Orji, *Cybersecurity Law and Regulation*, pp.17-19.

[10] *See* for *e.g.*, The African Union Convention on Cyber Security and Data Protection (Malabo, 2014) and the Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

2) International Cooperation

International cooperation implies the voluntary coordinated action of two or more countries occurring under a legal regime and serving a specific objective.[11] Within the context of cyber security, the concept broadly covers issues such as extradition and mutual legal assistance as well as general measures to ensure cross-border cooperation on cyber security issues. Such measures also include the sharing of information and resources either within a bilateral or multilateral framework with the aim of facilitating efficient responses to cyber threats.

3) Background on Africa

Africa comprises of 55 sovereign states and it is classified as the world's second largest and second most populous continent after Asia, with a terrestrial mass of 30, 2044, 049 million square kilometers and a human population of over one billion people.[12] The continent has five geographical sub-regions, comprising of: Southern Africa, Central Africa, East Africa, North Africa, and West Africa. The AU is the most prominent regional intergovernmental organization that unites African States and it comprises of 54 sovereign States with Morocco being the only sovereign State that is not a member of the union.[13] Some notable intergovernmental organizations that operate within Africa's sub-regions include: the COMESA[14] which comprises of 19 Member States, the ECOWAS[15] which comprises of 15 Member States, and the SADC[16] which comprises of 15 Member States.

2. THE AU CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION

The AU commenced the development of regulatory initiatives on cyber security towards the end of the last decade. A major factor that might have caused the AU's late development of cyber security initiatives could be traced to the low penetration of ICTs in Africa prior to the widespread proliferation of wireless technologies within the last decade. One of the first AU statements on the need to promote cyber security is found in the *AU Draft Report on a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation (2008)*.[17] The Report noted *inter alia* that emerging questions that needed to be addressed in the converged ICT environment include the "tracing and combating of cyber crime in all its forms (hacking, virus propagation, denial of service attacks, credit card fraud, etc)".[18] The Report also emphasized the need for the establishment of a harmonized regional policy and regulatory framework on cyber security.[19] Subsequently, on the 5th of November 2009, the AU Ministers in charge of Communication and Information Technologies convened an Extraordinary Session in Johannesburg, Republic of South Africa, where they

[11] *See The Blacks Law Dictionary* (8th Edition: West Group, 2004) p.359.

[12] *See* Matt Rosenberg, "Continents Ranked by Area and Population", <http://geography.about.com/od/lists/a/large.continent.htm>.[Accessed 25/03/2015]

[13] <http://www.an.int/en/member_states/country profiles>.

[14] <http://www.comesa.int/>.

[15] <http://www.ecowas.int/>.

[16] <http://www.sadc.int/>.

[17] *See* African Union, *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report* (African Union: Addis Ababa, Ethiopia, March 2008).

[18] *Id.*, p.49.

[19] *Id.*, p.75.

adopted a set of declarations known as the *Oliver Tambo Declaration*[20]. The Declaration directed the AU to "jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection"[21]. It also recommended that AU Member States should adopt the Convention by 2012.[22]

In 2011, the efforts of the AU and UNECA led the development of a draft framework on cyber security known as the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa.[23] The Draft Convention was subsequently adopted by the AU Expert Group on Cybersecurity in September 2012.[24] This was also followed by its approval by the 22nd Ordinary session of the AU Executive Council in January 2013. After that the Convention was to be presented for legal validation by the AU Justice Ministers conference in October, 2013,[25] after which it was to be presented for adoption by the AU Summit in January 2014 and opened for signatures and ratification by AU Member States. However, the Draft Convention could not be presented for the AU's adoption in January 2014 as a result of technical delays[26] and also due to opposition from the civil society and the academia. Several petitions by civil society groups and members of the academia were forwarded to the AU Commission to prevent the adoption of the Draft Convention following concerns that some of its provisions may harm the right to privacy and freedom of expression.[27] Other concerns included lack of wide consultations[28] and the absence of some critical governance mechanisms[29]. The Center for Intellectual Property and Information Technology Law (CIPIT) at the Strathmore University, Kenya led the opposition to the Draft Convention and also established an online petition to prevent its ratification.[30] Following these developments the Information Society Division of the AU Commission gave further room for the consideration of those concerns till May, 2014.[31]

[20] *See* Extra-Ordinary Conference of AU Ministers in Charge of Communication and Information Technologies, *Oliver Tambo Declaration* (Africa Union: Johannesburg, South Africa, 2-5 November, 2009).

[21] *See, Oliver Tambo Declaration*, p.4.

[22] *Id*.

[23] *See* Draft African Union (AU) Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, AU Draft0 010111, Version 01/01.2011.

[24] *See* UNECA Press Release, "Draft African Union Convention on Cybersecurity comes to its final stage", available at <http://www1.uneca.org/TabId/3018/Default.aspx?ArticleId=1931>. [Accessed 25/03/2015].

[25] *See* UNECA Press Release, "ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity", available at <http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislations-on-Cybersecurity.aspx> [Accessed 25/03/2015].

[26] *See* Craig Rosewarne and Adedoyin Odunfa, *The 2014 Nigerian Cyber Threat Barometer Report* (Wolfpack Information Risk and Digital Jewels: South Africa and Nigeria, April 2014) p.40.

[27] *See* Gareth Van Zyl, "Adoption of 'flawed' AU Cybersecurity Convention Postponed", IT Web Africa, (21 January 2014), available at <http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed> [Accessed 25/03/2015].

[28] *See* "Open Forum to discuss the proposed legal framework for cybersecurity in Africa", (July 26, 2013), available at <http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4> [Accessed 25/03/2015].

[29] *See* Uchenna Jerome Orji, "A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity", *Communications Law: The Journal of Computer, Media and Telecommunications Law*, (2012) Vol. 17, No.4, pp.128-130.

[30] The CIPIT's online petition is titled: *Stop the ratification of the African Union Convention on Cybersecurity*, available at<http://www.thepetitionsite.com/takection/262/148/817/>. *See also* Gareth Van Zyl, "Kenyan bid to stop 'flawed' AU Cybersecurity Convention", IT Web Africa (28 October 2013), available at<http://www.itwebafrica.com/security/513-africa/231821-keyan-bid-to-stop-flawed-au-cybersecurity-convention> [Accessed 25/03/2015].

[31] *See* Craig Rosewarne and Adedoyin Odunfa, *The 2014 Nigerian Cyber Threat Barometer Report*, p.40.

Later on 27th June 2014, the AU Heads of State and Government adopted a revised version of the draft Convention during the 23rd Ordinary Session of the AU Assembly in Malabo. The Convention which is known as the AU Convention on Cyber Security and Personal Data Protection[32] aims to harmonize the laws of African States on electronic commerce, data protection, cyber security promotion and cyber crime control. The Convention recognizes that cyber crime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa".[33] To a great extent, the Convention adopts a holistic approach to cyber security governance by imposing obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security. This approach apparently goes beyond that of the Council of Europe Convention on Cybercrime which focuses on the criminalization of cyber crimes and the establishment of procedural mechanisms for law enforcement and international cooperation.[34]

A. International Cooperation within the Framework of the AU Cyber Security Convention

Article 28 of the AU Cyber Security Convention establishes some provisions to facilitate international cooperation on cyber security.[35] It also requires AU Member States to make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) for the purpose of promoting cyber security and tackling cyber threats.[36] However, the extent to which the provisions of Article 28 can facilitate cooperation and mutual assistance amongst AU Member States appears to be limited. The Convention emphasizes the need for States to adopt the principle of double criminality (dual criminality)[37] when rendering cross-border assistance on cyber security issues without creating any mechanisms for Member States to fulfill extradition and mutual assistance requests in the absence of an extradition treaty or mutual assistance arrangement on the basis of dual criminality. Thus, Article 28: 1 of the Convention provides that: "State parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber crime will strengthen the possibility of regional harmonization of these measures and *respect the principle of double criminal liability*".[38] The application of the double criminality principle is also emphasized in Article 28: 2 of the Convention which provides that:

> "State parties that do not have agreements on mutual assistance in cyber-crime *shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal*

[32] *See* African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014). [Hereafter AU Convention on Cyber Security].

[33] *See* Preamble, AU Convention on Cyber Security.

[34] *See* Uchenna Jerome Orji, "Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection", *Computer Law Review International*, (October, 2014), Issue 5, pp.131-132.

[35] *See* Article 28 AU Convention on Cyber Security.

[36] *See* Article 28: 4, AU Convention on Cyber Security.

[37] "Double criminality" or "Dual criminality" exists where a conduct in issue have been criminalized in the laws of both the State requesting for assistance or extradition and the State from whom such assistance or extradition is requested. Under this principle, an extradition request can only be granted in accordance with an extradition treaty between two countries where both countries have criminalized the criminal conduct for which an extradition request is sought and the crimes are punishable by one year imprisonment or more. *See* ITU High Level Experts Group [HLEG] *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report* (ITU: Geneva, 2008) pp.14 and 56. *See The Blacks Law Dictionary* (8th Edition: West Group, 2004) p.537.

[38] *See* Article 28: 1, AU Convention on Cyber Security.

> *liability*, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis".[39]

Thus, the Convention appears to establish a blanket requirement for the application of the double criminality principle between Member States, without creating a legal basis or framework on which States while relying on the principle can base their extradition or mutual legal assistance requests in the absence of an existing international agreement between the requesting Member State and the Member State to whom such request is being made to. This state of affairs is further compounded by the absence of an AU legal instrument for the rendition of extradition or mutual assistance requests between Member States. The apparent problem here is that an AU Member State that may have adopted and ratified the Convention into its national laws may not have an extradition or mutual assistance treaty with another AU State that is also a party to the Convention. As such, a request for extradition or mutual assistance may not be successful between two Member States to the Convention even where the requirements of the double criminality principle have been fulfilled. This apparently implies that States after establishing "uniform" national laws that would guarantee the application of the double criminality principle would then have to individually establish mutual legal assistance treaties amongst themselves. As such, each Member State of the AU will have to establish mutual assistance treaties with the other 53 sovereign States of the AU. This will require each State to engage in tedious and expensive negotiation processes of which success may not always be guaranteed. For example, under the Convention a small AU State such as Cape Verde may only be able to obtain a regional wide guarantee for mutual assistance and extradition where it has entered into extradition or mutual legal assistance arrangements with all the 53 other sovereign States within the AU.

The above state of affairs also creates an enabling environment for forum shopping by cyber criminals within Africa. In this respect, a Member State that does not have extradition or mutual assistance arrangements with all other AU Members may technically provide a safe haven for cyber criminals since an extradition request cannot be successfully made to such State from another Member State with which it has no extradition treaty. This would further be compounded where such State does not have capacity to investigate or prosecute cyber crime or where it is reluctant to prosecute. In that that situation for example, a cyber criminal that operates from such State and whose acts have effects in another Member State with which the host State does not have an extradition treaty may not be held accountable. The same also applies where a cyber criminal commits an offence in a Member State and then flees to another Member State that does not an extradition treaty with the State in which the offence was committed. In both situations, the Member State where the cyber criminal is located may not even prosecute since there is no obligation to extradite. As such the doctrine of *aut dedere aut judicare* (extradite or prosecute) would not apply.

The position is quite different under the Council of Europe (CoE) Convention on Cybercrime which establishes very elaborate procedures to facilitate international cooperation amongst Member States. Thus, while extradition principles established under article 24 (1) of the CoE Convention on Cybercrime provide that extradition arrangements between Member States shall be based on the principles of "dual criminality" (double criminality), Member States are

[39] *See* Article 28: 2, AU Convention on Cyber Security.

however allowed to adopt the Convention as a legal basis for extradition proceedings in the absence of a treaty on extradition. This apparently recognizes the fact that extradition treaties may not exist between all Member States to the Convention. In this respect, article 24(3) of the CoE Convention provides thus:

> "If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article".[40]

The Convention also provides that where a Member State refuses to grant an extradition request, that such Member State shall prosecute the offender at request of the Member State whose extradition request was refused.[41] Thus, the Convention entrenches the doctrine of *aut dedere aut judicare*. The Convention also recognizes the application of the double criminality principle in mutual assistance requests between Member States.[42] However, the Convention also establishes procedures for a Member State to render mutual assistance requests to another Member State where there is no existing international agreement or arrangement between them on the basis of a uniform or reciprocal legislation.[43] The Convention's international cooperation procedures are not meant to supersede the provisions of existing international agreements or reciprocal arrangements on mutual assistance and extradition[44] and neither are such procedures intended to create a separate general regime for mutual assistance that is parallel to the European Convention of on Mutual Assistance.[45] Nevertheless, the procedures provide a regime for international cooperation between Member States that lack such international cooperation arrangements and thus reducing impediments to international cooperation to the barest minimum.

3. COOPERATION UNDER AFRICAN SUB-REGIONAL LEGAL INSTRUMENTS ON CYBER SECURITY

A. The ECOWAS Directive on Fighting Cybercrime

In August 2011, the ECOWAS Council of Ministers adopted the Directive C/DIR.1/08/11 on Fighting Cybercrime at its Sixty Sixth Ordinary session at Abuja.[46] The Directive imposes obligations on Member States to criminalize cyber crime[47] and also establishes a framework to facilitate international cooperation on cyber security. In this respect, article 33(1) of the Directive provides that:

> "Where Member States are informed by another Member State of the alleged commission of an offence as defined under the Directive, such Member States "*shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence*".[48]

[40] *See* Article 24(3) CoE Convention on Cybercrime.
[41] *See* Article 24(6) CoE Convention on Cybercrime.
[42] *See* Article 25(5) CoE Convention on Cybercrime.
[43] *See* Article 27 CoE Convention on Cybercrime.
[44] *See* Explanatory Note, CoE Convention on Cybercrime, No.244.
[45] *See* Explanatory Note, CoE Convention on Cybercrime, No.262-263.
[46] *See* ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).
[47] *See* Article 2 ECOWAS Directive on Cybercrime.
[48] *See* Article 33(1) ECOWAS Directive on Cybercrime.

The Directive also provides that "such cooperation shall be carried out in line with relevant international instruments and mechanisms on international cooperation in criminal matters"[49]. Applicable ECOWAS instruments on international cooperation include: the ECOWAS Convention on Mutual Assistance in Criminal Matters[50] and the ECOWAS Convention on Extradition.[51]

The ECOWAS Convention on Mutual Assistance in Criminal Matters establishes a broad framework for the rendition of mutual assistance amongst ECOWAS States where there is an absence of applicable international agreement between them on the basis of a reciprocal legislation. Under the Convention, Member States are required to afford each other "the widest measure of mutual assistance in proceedings or investigations in respect of offences the punishments of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Member State".[52] Thus, within the framework of the Convention, every ECOWAS Member State has an obligation to render mutual assistance to all other ECOWAS States where such assistance is requested with respect an offence that constitutes a crime in both the requesting and requested Member States[53], regardless of the absence of an applicable bilateral mutual assistance agreement between the requesting and requested Member States.

The ECOWAS Convention on Extradition also establishes a broad framework for the rendition of extradition requests between ECOWAS Member States. Thus, the Convention requires Member States to render extradition requests on the basis of dual criminality regardless of the absence of a bilateral extradition treaty between the requesting and requested Member States.[54]

Accordingly, the existence of the above ECOWAS Conventions on mutual assistance and extradition creates a broad framework on which ECOWAS Member States that have established cyber security laws can render mutual assistance and extradition requests to other ECOWAS States on the basis of dual criminality and regardless of the absence of applicable bilateral mutual assistance or extradition treaties.

B. The COMESA Model Cybercrime Bill

In October 2011, the COMESA established a Model Cybercrime Bill[55] to provide a uniform framework that would serve as a guide for the development of cyber crime laws in Member States, however, the Bill does not establish any binding obligations on Member States to criminalize cyber crimes. The Bill largely adopts the language and model of legal instruments such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation. It also establishes an elaborate guide for the development of general framework to facilitate international cooperation[56], extradition[57], and mutual assistance[58] and provides

[49] *See* Article 33 (2) ECOWAS Directive on Cybercrime.

[50] *See* ECOWAS Convention on Mutual Assistance in Criminal Matters (A/P1/7/92) (29 July, 1992, Dakar, Senegal).

[51] *See* ECOWAS Convention on Extradition (A/P1/94) (6 August, 1994, Abuja, Nigeria).

[52] *See* Article 2(1) ECOWAS Convention on Mutual Assistance in Criminal Matters.

[53] *See* Article 2(1) ECOWAS Convention on Mutual Assistance in Criminal Matters.

[54] *See* Articles 2 and 3 ECOWAS Convention on Extradition.

[55] *See* Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

[56] *See* section 41 COMESA Model Cybercrime Bill.

[57] *See* section 42 COMESA Model Cybercrime Bill.

[58] *See* section 43 COMESA Model Cybercrime Bill.

for the establishment of national 24/7 points of contact.[59] However, despite its framework on international cooperation, the Bill only serves as a mere guide or model for development of national cyber security laws in Member States. Thus, the Bill does not establish any international cooperation obligations on Member States and neither can it be used as a legal instrument for cooperation amongst Member States. Also unlike the ECOWAS, the COMESA does not have any existing legal frameworks to facilitate mutual assistance and extradition among Members. As such, COMESA Member States that have used the Bill to develop their national laws would still have to enter into separate bilateral arrangements with other Member States in order to obtain any form of international cooperation or mutual assistance.

C. The SADC Model Law on Computer Crime and Cybercrime

In March 2012, the SADC adopted the Model Law on Computer Crime and Cybercrime[60] to serve as a guide for the development of cyber security laws in SADC Member States. However, it does not impose any obligations on Members to establish cyber crime laws. It does not also establish any provisions to guide the development of international cooperation regimes in Member States and neither does it establish any international cooperation obligations on Member States. However, Members that have established cyber security laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters[61] and the Protocol on Extradition[62] to obtain international cooperation from other Members. Under the SADC Protocol on Mutual Assistance, Member States are required to provide each other with "the widest possible measure of mutual legal assistance in criminal matters"[63]. The Protocol also requires that such assistance shall be rendered without regard to whether the conduct which is the subject of the mutual assistance request by a Requesting State would constitute an offence under the laws of the Requested State.[64] On the other hand, the Protocol on Extradition requires that SADC States can only obtain cooperation amongst themselves on the basis of dual criminality.[65]

4. PROPOSALS TO STRENGTHEN INTERNATIONAL COOPERATION ON CYBER SECURITY AMONGST AFRICAN STATES

The review in section 2 of this paper has shown that the AU Cyber Security Convention does not provide an adequate framework for international cooperation and mutual assistance amongst African States. The review in section 3 showed the existence of international cooperation and mutual assistance mechanisms within two African sub-regional groupings, the ECOWAS and the SADC. Consequently, Africa has a situation whereby there is no regional wide cooperation and mutual assistance on cyber security, thus resulting in the limitation and fragmentation of cooperation and mutual assistance along sub-regional and bilateral arrangements. While it is agreed that cyber threats that affect African States may also emanate from outside the continent, which also underscores the need for wide international cooperation amongst all States, however

[59] *See* section 52 COMESA Model Cybercrime Bill.

[60] *See* SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

[61] *See* SADC Protocol on Mutual Legal Assistance in Criminal Matters (Luanda, 3 October, 2002).

[62] *See* SADC Protocol on Extradition (Luanda, 3 October, 2002).

[63] *See* Article 2(1) SADC Protocol on Mutual Legal Assistance in Criminal Matters

[64] *See* Article 2(4) SADC Protocol on Mutual Legal Assistance in Criminal Matters

[65] *See* Article 3 SADC Protocol on Extradition.

the development of a framework for such global cooperation is beyond the AU and also beyond the scope of this paper. This notwithstanding, AU Member States should at least be able to obtain international cooperation amongst themselves to the widest possible extent. Thus, since the AU Cyber Security Convention is meant to serve as a treaty for the promotion of cyber security within Africa, the ideals of African unity and cooperation which inspired the founding of the AU[66] would not have been fulfilled if there is no explicit AU framework to facilitate international cooperation and mutual assistance amongst Member States. The Convention's emphasis on the use of existing channels of cooperation or bilateral or multilateral arrangements only narrows cooperation to multilateral or sub regional or bilateral arrangements, and thus resulting in a fragmentation of cyber security cooperation within Africa. Consequently, the absence of a broad AU framework to facilitate mutual assistance and international cooperation would limit the effectiveness of the Convention.

To address above state of affairs, it may be necessary for the AU to establish an additional protocol that would create provisions enabling all Member States to the AU Cyber Security Convention to adopt the protocol as a legal basis for the rendition of international cooperation such as extradition requests or mutual assistance in accordance with the principle of dual criminality where there is an absence of applicable treaties between Member States. The AU may also consider the establishment of explicit extradition and mutual assistance instruments to facilitate the rendering of extradition and mutual assistance requests within the African region with respect to cyber crime offences established under the Convention. This type of mechanism already exists in Europe in form of the European Convention on Extradition[67] and the European Convention on Mutual Assistance in Criminal Matters[68] which are also applicable under the Council of Europe Convention on Cybercrime.[69]

The AU Convention does not create a regional Computer Emergency Response Team (CERT) to facilitate cyber security efforts and coordinate responses to cyber security incidents at the regional level. Rather, article 28:3 of the Convention imposes obligations on Member States to "encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs)".[70] This provision is unique as there are no African sub regional cyber security instruments that require Member States to promote the establishment of a national CERT or CSIRT. However, the need for the establishment of a regional CERT or CSIRT is also imperative as its absence may result in poor cooperation or coordination of African cyber security efforts and responses to cyber threats at the regional level. In this respect it should be noted that a regional CERT has a broader scope of functions and responsibilities than a national CERT. A national CERT is usually responsible for coordinating emergency responses to cyber threats affecting national computer or information systems and

[66] *See* Article 3 Constitutive Act of the AU (July, 2000).

[67] *See* the European Convention on Extradition (Paris, 13 December 1957) [ETS No. 24].

[68] *See* the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 20 April 1959) [ETS No. 30]. See also the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, (Strasbourg, 17 March 1978) [ETS No. 99].

[69] *See* Article 39 Council of Europe Convention on Cybercrime.

[70] *See* Article 28: 3, African Union Convention on Cyber Security and Personal Data Protection

also establishing best practices relating to the use of such systems within a State.[71] On the other hand, a regional CERT may perform the functions of a national CERT at a regional level and also facilitate cyber security cooperation between national CERTs.

There have been some efforts within the African information security industry to develop a CERT for Africa. However, although such industry initiatives have a great potential to enhance private sector participation in African cyber security, they may not be adequate for the purpose of coordinating national responses to cyber security or fostering cooperation amongst Member States. A legal basis may be found for the establishment of a network security agency within the AU framework under article 32 of the Convention which provides for an operational mechanism for the Convention. Some of the functions of the Convention's operational mechanism include:

a) Promoting the adoption and implementation of measures to strengthen cyber security in electronic services and combating cyber crime and human rights violations in cyberspace;
b) Advising African governments on measures to promote cyber security and combat cyber crime; and;
c) Analyzing the criminal behaviors of cyberspace users within Africa and transmitting such information to competent national authorities.[72]

Apparently, the above mandate may be broadly interpreted to create a regional network agency which is similar to the European Information Security Agency (ENISA). The ENISA was established in 2004 by the European Commission[73] to promote cyber security and critical information infrastructure protection. The Agency serves as a center of excellence for Member States of the European Union and European institutions on cyber security issues. Its responsibilities include providing advice and recommendations on cyber security and disseminating information on standards for best practices.[74] A regional network agency that is established under article 32 of the Convention may also function as a regional CERT where its mandate is enlarged to function as such. However, the establishment of an AU CERT would not be without some peculiar challenges such as lack of funding, differences in the legal systems of AU Members, and the ability of Member States to effectively cooperate in sharing information and critical resources. Some of such challenges were faced by the EuroCERT.[75]

CONCLUSION

The adoption of the AU Cyber Security Convention marks a significant milestone in African cyber security governance and underscores Africa's efforts to promote the development of a secure information society. This notwithstanding, the success of the Convention, to a great extent, will not only be determined by the number of AU Member States that eventually ratify the Convention, but also by the extent to which it can serve as a viable legal instrument for cyber

[71] The responsibilities of a national CERT include: detecting, identifying or monitoring threats to cyber security and issuing early warnings of such threats; and publicizing best practices and guidance for incident response and prevention. *See* ITU Study Group Q.22/1, *Report on Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts* [Draft] (ITU-D Secretariat: Geneva, January 2008) p. 39/71.

[72] *See* Article 32 African Union Convention on Cyber Security and Personal Data Protection

[73] *See* Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency.

[74] *See* <http://www.enisa.europa.eu/>.

[75] *See* ENISA, *CERT Cooperation and its further facilitation by relevant Stakeholders* (ENISA, 2006,) pp.23-25.

security cooperation amongst Member States. However, despite its seeming comprehensive approach to cyber security governance, the Convention in present form offers no hope for broad international cooperation amongst all AU States. Consequently, there is need for the AU to consider the issues raised in this paper in order to prevent the limitation or fragmentation of Africa's cyber security cooperation to only bilateral arrangements or to sub-regional arrangements under the ECOWAS and SADC frameworks.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT

Richard Hill
Hill & Associates
Geneva, Switzerland
rhill@hill-a.ch

Abstract: The cyber security situation is not as bad as most people think it is – it is worse than most people imagine it could be. Indeed the lack of security of the Internet and of the devices connected to it results in serious vulnerabilities. These vulnerabilities create risks for infrastructures that increasingly rely on the Internet, including not just communications, but also power generation and distribution, air transport, and, in the near future, road transport. It is easy and relatively inexpensive to access cyberspace and to obtain the means of conducting offensive cyber attacks. Thus it is tempting to develop offensive cyber capabilities and indeed some states are doing so – as published in their national cyber security strategies, and several states have allegedly carried out cyber attacks. At the same time, a state is bound to protect its citizens, including against cyber attacks and cyber warfare. This will become increasingly difficult, if not impossible, if current trends continue unchecked. This article argues that international agreements on improving cyber security, and limiting cyber attacks would appear to be necessary and appropriate measures. Yet key developed countries resist taking legally binding measures of that nature, see in particular the discussions and outcome of the 2012 International Telecommunication Union (ITU) World Conference on International Telecommunications (WCIT). On the contrary, some of these countries practice mass surveillance, which some consider to be a threat to citizens and to the security of states, and which some authors have even considered, figuratively, to be a form of cyber war, even if it is inappropriately justified as a means of combating terrorism. And they resist calls to end mass surveillance. This paper argues that the positions taken by key developed countries could have grave negative consequences in the future, in particular for those very countries. The time has come to take steps to prevent this, which include more discussions and engagement in various forums, including ITU.

Keywords: *cyber security, cyber warfare, ITRs, ITU, WCIT*

1. INTRODUCTION

Cyber security can be defined as the collection of tools and procedures that ensure availability, integrity, authenticity and confidentiality of information and communications.[1] Both computer systems and networks can be attacked to prevent their use (denial of service), to compromise and alter the data they store or transport, to compromise ("spoof") the identification of the originator, and to read data without authorization (eavesdropping). In this paper, we will refer to all such attacks as cyber attacks.

The structural and technological changes arising from telecommunications privatization, liberalization, and the growth of mobile and Internet Protocol based networks (the Internet) have resulted in a degradation of network security (and consequent facilitation of cyber attacks), increasing cyber crime, proliferation of viruses, worms and other malware, and proliferation of spam (Talbot, 2006; WGIG, 2005, para. 17-18; Deibert, 2013; Brunton, 2013; Hill, 2014). And the situation will get worse, not better (Jeffers, 2013). In particular, as discussed in some detail below, confidentiality is not ensured, due to mass surveillance.

It is worth outlining the key reasons for this situation. The Internet was initially deployed to connect a handful of large, expensive computers operated by a small group of trusted entities. Security was not a major design goal: security was achieved by securing the end-devices connected to the network. The situation changed dramatically with the emergence of personal computers, whose security is mostly very weak (despite attempts by manufacturers to improve the situation) and with the connection of those insecure devices to the Internet (Hill, 2014, pp. 24 and 32). As Robert Khan, co-creator of Transmission Control Protocol/Internet Protocol (TCP/IP), puts the matter (Khan, 2011): "At present, the Internet environment is tilted in favor of those with adverse motives, while the rest of the community must be on constant vigil to defend against harmful interference."

It is well known that the cost of entry into cyber space is relatively low (Schreier, 2015, p. 12) and that cyber capabilities are relatively inexpensive: with a computer and Internet access anyone can engage in cyber attacks, and many states can even envisage cyber warfare (Lewis, 2010, p. 2; Schreier, 2015, pp. 26 and 27). It is important to note here that there are differing definitions of the term "cyber warfare", resulting in different understandings of consequences and preventive measures. Strictly speaking, it refers to massive state-organized assaults, akin to conventional warfare, but it is also used more generally. Indeed, the term "war" is often used figuratively, as in economic war (Freeman, 2015), the war on drugs, and the war on terrorism. The Inter-Parliamentary Union has recently adopted a resolution that states (Inter-Parlimentary Union, 2015): "Considering that cyber warfare may encompass, but is not necessarily limited to, operations against a computer or a computer system through a data stream as a means and method of warfare that is intended to gather intelligence for the purpose of economic, political or social destabilization or that can reasonably be expected to cause death, injury, destruction or damage during, but not exclusively in, armed conflicts". A recent academic work uses "cyber war" figuratively to refer to utilization of digital networks for geopolitical purposes, including covert attacks against another state's electronic systems, but also the variety of ways the Internet is used to further a state's economic and military agendas (Powers and Jablonsky, 2015). But

[1] This is a simplified version of the definition found in Recommendation ITU-T X.1205 and it is consistent with other older definitions of security, such as that found in Recommendation ITU-T E.408.

this figurative use of the term “cyber war” predates academic writings, see for example an article by a former director of the US National Security Agency (McConnell, 2010). We note that the figurative use of the term is consistent with what is found on the web sites of some private companies active in the area (Rand, 2015). But it has also been said that the figurative use of the term is inappropriate, see Singel (2010), who quotes the US “cyber security czar”.

Various states have been accused of practicing cyber espionage or even of conducting cyber attacks. Not surprisingly, the USA accuses China (Sanger, 2013) and Russia (AP, 2011) of actively engaging in cyber attacks or at least in commercial cyber espionage. However, it is generally accepted that the USA and Israel conducted an apparently successful secret cyber attack on Iranian nuclear facilities, through the Stuxnet virus (Sanger, 2012), and that the US has invested significantly in cyber espionage (Gellman and Miller, 2013; Poulsen, 2015) and in offensive and defensive cyber capabilities (Harris, 2015). Separately, Chinese government researchers have published in the open literature accounts of some of their work (Stone, 2013).

It is generally agreed that conventional laws apply online as well as offline[2], so certain types of cyber attacks are surely illegal. However, this paper argues that additional agreements are needed regarding cyber operations: if there is no common agreement regarding the appropriate level of cyber operations by states, then cyber attacks may become more common and could escalate out of control. In particular, mass surveillance programs may become more widespread and more intensive. The paper argues that there should be some agreement on how to respond appropriately to cyber attacks, and how to distinguish the responses to cyber attacks originating from states, from commercial organizations, or from criminal organizations.

Concern regarding the lack of security of the Internet is widespread (Talbot, 2006). Vint Cerf, Khan’s TCP/IP co-creator, agrees that a change is needed (Cerf, 2011): “We can’t let it sit the way it is now, it is simply not adequate. We’re depending too heavily on the Internet, for too many different things to allow it not to be evolved to a more secure state.” As Schreier (2015, p. 14) puts the matter: “modern society’s overwhelming reliance on cyberspace is providing any attacker a target-rich environment, resulting in great strain on the defender to successfully defend the domain”. That is, the situation regarding cyber threats is not as bad as most people think it is: it is worse than most people could imagine it could be.

Unless limits are internationally agreed, state-led cyber attacks threaten the trust required among stakeholders for effective internationally agreed cyber security goals, such as security of electronic commercial transactions and privacy of personal communications. The establishment of trust through agreed limits in state-led cyber attacks and agreed ways to respond to cyber attacks (whether originated from states, commercial organizations, or criminal organizations) could be achieved through increased international cooperation. Increased international cooperation could also facilitate the development and implementation of appropriate technical measures to improve cyber security, which might include greater use of encryption (Internet Architecture Board, 2014), and stronger encryption.

Indeed, the 2013 Seoul Conference on Cyberspace stressed the benefits of such international cooperation (Seoul Conference, 2013). Richard Haass, President of the Council on Foreign

[2] For example, UN General Assembly Resolution A/RES/68/167 “*Affirms* that the same rights that people have offline must also be protected online, including the right to privacy”. And there is a long line of court decisions applying conventional law to the Internet (Hill, 2014, p.18).

Relations, suggests (Haass, 2010): "Cyber is exactly at the point today where nuclear was maybe 50 years ago, where people are beginning to think, what sort of rules do we set up? What sort of arrangements do we put into place?" The East West Institute's 2012 Cybersecurity Summit called for greater collaboration on cyber security between both the private and public sectors and international actors, noting (East West Institute, 2012): "securing cyberspace is a global challenge – one that cannot be solved by a single company or country on its own." And no doubt it cannot be solved by a single instrument, or type of instrument, either: a combination of voluntary codes of conduct, soft law, and law at both the national and international levels will likely be required.

Similar concerns and calls for cooperation are found in international agreements such as Resolution 130 of the ITU, which recites various threats and trends and notes "the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memorandums of understanding, etc)". Calls for cooperation and action are also found in ITU World Telecommunication Standardization Assembly (WTSA) Resolutions 40 and 52.

In this light, it is not surprising that the matter of improving cooperation regarding cyber security was discussed at the ITU's 2012 WCIT. WCIT-12 was convened in December 2012 at the request of the ITU members in order to revise the International Telecommunication Regulations (ITRs), a treaty which had been agreed in 1988 and which opened the way for the privatization and liberalization that has since characterized the telecommunications sector (Hill, 2013; Hill, 2013b).

The purpose of the ITRs is to establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services. The ITRs provide the groundwork from which the ITU promotes the development of telecommunication services and their most efficient operation while harmonizing the development of facilities for worldwide telecommunications.

The issue of Internet security had already surfaced in 1988 at the ITU's World Administrative Telegraph and Telephone Conference (WATTC), which was the predecessor of WCIT and which approved the 1998 version of the ITRs. When the WATTC was convened on 28 November, the Morris Internet worm (Eisneberg et al., 1989) was still a topic of concern. Although the worm itself was not explicitly mentioned in the ITRs, the "avoidance of technical harm" provision of Article 9 is generally considered to have been inspired by a desire to take steps that would prevent a reoccurrence of problems of this type (Hill, 2013b, p. 8). This is possibly the first treaty provision dealing with the security of telecommunication networks, a form of cyber security[3]. A similar provision was subsequently added to what is now Article 42 of the ITU Convention[4]. In

[3] Actually the original predecessor of the ITRs, the 1865 treaty that created the ITU, included a provision regarding the use of encryption, and such provisions are also found in later versions. But those provisions were as much about costs (they prevented the use of private short-codes which reduced the number of words in a telegram) as about national security, so they cannot be considered to be security provisions in the modern sense of the term. See Headrick (1991).

[4] A detailed discussion of the evolution over time of provisions related to security in the various instruments of the ITU (including the "technical harm" provision of Article 9 of the ITRs) is given in Rutkowski (2011).

the author's opinion, those provisions have not had any significant practical effect, but this does not necessarily mean that new provisions agreed today would not be effective.

2. DISCUSSIONS AT WCIT

A. Preparations for WCIT

Some of the proposals submitted to WCIT were motivated by an underlying goal to increase sovereign control over some portions of the Internet (indeed a late submission from the Russian Federation explicitly called for that – this proposal was never placed on the agenda so it was not discussed at the conference (Hill, 2013b, pp. 60-62)). Such proposals must be seen in light of a perceived erosion of national control and a perceived domination of the Internet by the United States and its dominant private companies (Hill, 2013c). Be that as it may, some of the proposals could have facilitated state control over some aspects of the Internet, including censorship. This understandably raised concerns in many quarters and resulted in unbalanced press coverage which stressed those proposals while ignoring the many other proposals which addressed commercial matters, such as reduction of mobile roaming prices, transparency of pricing in general, etc. (Hill, 2013b, pp. 35-48 and 65-66; and 59 and 63, respectively). Several of the pro-consumer provisions were supported by developing countries but opposed by developed countries (Hill, 2013b, pp. 59-63).

The issues of security and spam had long been discussed in various ITU meetings[5]. Thus it was not surprising that various proposals were presented to WCIT regarding security and spam. All called for increased international cooperation, but differed in other respects. Some of the proposals were characterized as more-or-less disguised attempts to impose or to favor censorship (see below), but the true intent of the more elaborate proposals was to likely limit state-sponsored cyber attacks (Mueller, 2012; Hill, 2013b, pp. 41-42)[6]. The USA made it clear that it was opposed to any text on security or spam in the ITRs[7], refusing even to consider a proposal that was essentially copy-pasted from one of USA President Obama's Presidential Declarations[8]. While some European and other countries were initially willing to consider some text related to security and spam (Hill, 2013b, pp. 29 and 33), the USA was successful in influencing their positions with the result that there were strong differences of views going into the conference (Hill, 2013b, p. 54). The main reason given by the USA for opposing cooperation to improve security and combat spam was a concern that a treaty provision to that effect could be used by authoritarian countries to justify censorship or other restrictions on freedom of speech or human rights (Majority Committee Staff, 2012; Rizo, 2012; US Congress, 2012).

[5] For example, Resolution 130 "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies" has been revised at every Plenipotentiary Conference since it was adopted in 2002; cyber security and spam have been topics of study in ITU-T Study Group 17 since, respectively, 2001 and 2009.

[6] Hill (2013b, p. 42) concludes, on the basis of a legal analysis of the proposals and the ITU Constitution, that a Russian proposal could be construed as an attempt to authorize blocking of state-originated cyber attacks, and to bind all states to cooperate to prevent transmission of such cyber attacks.

[7] See WCIT document 9 "United States of America Proposals for the Work of the Conference", August 3, 2012, which notes that cyber security should be treated by member states primarily as a sovereign issue, and opposes "any effort to interfere with those rights."

[8] See ITU documents CWG-WCIT12/C-60 for the proposal, and CWG-WCIT12/TD-62 for the US opposition, expressed as "cybersecurity should not be included in the ITRs in any way, shape or form." The proposal is CWG/4/225 in the publicly-available "Draft of the future ITRs" <http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf>

However, a legal analysis of the ITRs does not support the allegation that it could threaten freedom of speech (Hill 2013; Hill 2013b)[9], see below. And the USA's arguments appear incongruous in light of its pervasive domestic and foreign surveillance – as Brazilian President Dilma Rousseff has pointed out: "In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy" (Borger, 2013)[10] –, and that at least some of the foreign surveillance appears to be done without meaningful judicial oversight (Hill, 2013c; National Security Agency, 2013; Bowden, 2013). Be that as it may, the discussions at WCIT were difficult.

B. Outcome of WCIT

Strong objections were raised by the USA regarding certain proposed provisions of the new treaty (Hill, 2013; Hill, 2013b). These objections were supported to some extent by other countries and resulted in the preparation of a compromise text (Hill, 2013b, pp. 55-65). The compromise text was acceptable for most countries – albeit not for the USA – (Hill, p. 54) but, at the last minute, a vote was called to introduce a controversial provision in the preamble of the treaty. That provision was not related to security or spam, it was related to unilateral actions by some countries to block access by other countries to certain web sites (Hill, 2013b, p. 65). The inclusion of that controversial provision in the preamble resulted in most developed countries refusing the sign the treaty, on the grounds that they needed more time to consider the implications of the provision in question. In what follows, we will focus only on the provisions regarding security and spam since these appeared to be acceptable to a majority of states; a full account of the discussions and issues regarding the other provisions is found in Hill (2013b).

The treaty provisions approved at WCIT include two new articles on security and spam. These articles state:

> "6: Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public."

And

> "7: Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense."

These articles have been heavily criticized in the USA, in particular in relation to freedom of speech (Hill, 2013; Hill, 2013b, p. 70, footnote 5). However that criticism is not valid from a legal point of view, in particular because the Preamble and Article 1 of the treaty make it clear that these provisions cannot be invoked to justify restrictions on freedom of speech (Hill, 2013; Hill 2013b, pp.86-89). In the author's view, the real motivation for the USA resistance to article 6 appears to be a desire to avoid international agreements on improving cyber security, as such agreements might restrict the USA's ability to carry out cyber attacks and mass surveillance (Hill, 2013b). For example, apparently no judicial approval is required in some cases for surveillance of non-US persons; this was not publicly known when WCIT took place and presumably would have had to be revealed in the context of cooperation on cyber security matters; such practices might have been found objectionable by some countries (Hill, 2013b, p. 42). As noted above,

[9] The author is not aware of any other peer-reviewed legal analysis and has been told privately by both legal scholars and representatives of certain states that his analysis is sound.

[10] The same point is made in paragraph 14 of High Commissioner for Human Rights (2014)

most of the states that did not sign the treaty referred to the new clause in the preamble as the main reason for not signing. One can speculate regarding other reasons, which might be similar to those posited above for the USA. And one can speculate that, at the time, the US has greater cyber capabilities than other countries (Harris, 2014), so other countries were more willing to accept restrictions.

As noted above, lack of security favours cyber attacks and mass surveillance is a form of cyber attack (and, figuratively speaking, perhaps even cyber war). Consequently, as Schreier (2015, p. 7) puts the matter: "In fact, there is a stunning lack of international dialogue and activity with respect to the containment of cyber war. This is unfortunate, because the cyber domain is an area in which technological innovation and operational art have far outstripped policy and strategy, and because in principle, cyber warfare is a phenomenon which in the end must be politically constrained."

A continuing resistance to improve cyber security and to curtail mass surveillance could have negative consequences for the Internet (Naughton, 2013; Morozov, 2013). Mass surveillance is often justified as a means to combat terrorism. But the number of potential terrorists present in developed countries is very small, so from a statistical point of view a mass surveillance program cannot be effective at detecting them: there will be too many false positives (Rudmin, 2006). However, mass surveillance programs can collect information that is useful for economic and political purposes, and reportedly some countries are using them for such purposes (Poitras, Rosenbach and Stark, 2013; Gellman and Miller, 2013; CBS News, 2014; Price, 2014; Tribune de Genève, 2015[11]). Thus, figuratively, mass surveillance can be viewed as a form of cyber warfare, even if it is not cyber warfare in the legal sense of the term. And calls to continue it are not justified: mass surveillance violates human rights, and it is not effective (Harding, 2015; Powles, 2015). Nobody would accept to put mass surveillance into place to prevent violent bank robberies, because everybody can see that it would not be effective. The same holds for the terrorist threats in developed countries, which share many of the characteristics of violent crime.

3. THE FUTURE

A persistent refusal by developed countries to envisage cooperation with developing countries and emerging economies on terms that are acceptable to them to improve cyber security might have undesirable consequences. For sure there are many cooperation mechanisms and it is easier to negotiate non-binding agreements. But non-binding agreements are just that, and forums that do not include all states tend to make decisions that are consistent with the interests of the participating states, but not necessarily with the interests of non-participating states. In the absence of global agreements, states may choose to enter into bilateral or regional arrangements. At present, it is impossible to say whether those bilateral or regional arrangements might set the stage for future global agreements, or whether they might be detrimental to the global interconnectivity of today's telecommunications systems. As a Canadian think-tank put the matter referring to overall governance, which includes the security issues outlined above (Raymond and Smith, 2013):

[11] Citing a proposed new French law that would authorize certain types of surveillance in cases of major economic or scientific interests, as well as national defense, prevention of terrorism, etc.

> “the larger problem [of the split between signatories and non-signatories of the 2012 ITRs] in the long term is the overall degree of complexity introduced into the governance of international telecommunications, the potential for increased transaction costs and the eventual possibility of significant divergence between the two treaty regimes over time. Given the similarity between the two treaties [1988 versus 2012], as well as the long history of routine cooperation on international telecommunications and the resulting business relationships and accumulated social practice, there are reasons to believe that this complexity may be manageable, if suboptimal. This assessment may not apply, however, in the event that the parties to the new ITRs engage in subsequent negotiations, building on the accompanying resolutions to erect a parallel institution for Internet governance. … Further, since routing is currently done without regard for international borders, the existence of parallel Internet governance regimes that may evolve with very different privacy protections poses challenging questions about the sustainability and desirability of legacy routing practices.”

Cyber security issues are only one part of the overall governance of international telecommunications. But they are an important part (Eichensehr, 2014). And if there is uncertainty regarding global governance, then it is difficult to predict how the situation will evolve with respect to cyber security. On the one hand, private companies appear to favor improved cyber security in the interests of their customers, for example by improving encryption (McCarthy, 2015). On the other hand, some states appear to resist those improvements, because they are of the view that mass surveillance is an effective means to protect their citizens (United States of America, 2014; Ball, 2015; McCarthy, 2015; Sanger, 2015). In the absence of international agreements, the most likely outcome would appear to be the emergence of a “federated Internet”: one in which national networks are interconnected, but remain under local control to some extent. This is already largely the case for China, and for the internal networks of large private companies. A more detailed discussion of this scenario is given in Hill (2015).

Despite rhetoric to the contrary, the USA government supports greater state involvement in improving cyber security. Similarly, former CYBERCOM and NSA Director Keith B. Alexander has argued that securing private networks cannot be achieved through voluntary mechanisms alone (Alexander, 2012): “Recent events have shown that a purely voluntary and market driven system is not sufficient. Some minimum security requirements will be necessary to ensure that the core, infrastructure is taking appropriate measures to harden its networks.” Indeed, state involvement can be justified in light of the externality effects of security – or rather, lack of security – which effects are well explained by Schneier (2007). While it has proven possible to reach agreements to limit certain types, or certain uses, of conventional weapons, it is not clear whether it will be possible to reach similar agreements regarding cyber attacks (Eichensehr, 2014).

Some may take the view that there is no need for a treaty regarding cyber security or even international telecommunication matters in general: any matters requiring inter-governmental coordination can be handled by soft-law, or bilateral or regional agreements. But the divergence of views expressed at WCIT indicates that there is a need to agree some basic principles at a high level even if it is not clear which, if any, to enshrine formally in a treaty (Eichensehr, 2014). In the author's view, lack of treaty-level agreement regarding cooperation with respect to network security issues in effect favors the current practices of secret (and unacknowledged) cyber attacks and mass surveillance, because there are no agreements on how to interpret and to apply existing international law. In particular, the USA takes the view that its obligations under international human rights law with respect to privacy do not apply to non-USA persons (United States of America, 2014). Treaty-level agreements would presumably affect such activities, because treaties should be enacted into national law, which laws would be enforced nationally (but it should be noted that treaties are not always respected).

International agreements to improve cyber security would likely make mass surveillance more difficult, if not impossible. Agreements could be envisaged for many different aspects, for example to allow pervasive strong encryption[12]. It will surely be difficult to discuss all topics at the same time, and to envisage their inclusion in a single instrument. Thus a first step could be an agreement in principle to cooperate and to agree on forums in which to carry out more detailed discussions in line with some agreed principles, for example, limits on mass surveillance, and limits on the means used to carry out authorized surveillance.

Reportedly, states whose private companies are producers of telecommunications hardware have programs in place to intercept some shipments of such hardware so that the hardware can be modified to facilitate monitoring of communications and even to allow the hardware to be attacked (Greenwald, 2014; Paganini, 2014). Such modifications might escape detection by the end-user and might enable monitoring or attacks even if the hardware is used for a private network that is not connected to the public Internet[13] (Perlroth and Sanger, 2015; Kaspersky Lab, 2015). Thus, nobody can ensure secret communications unless they manufacture their own hardware and software. But this is beyond the reach of all but a few states. Further, sophisticated techniques can be used to implant spyware no matter who manufactured a system (Gallagher and Greenwald, 2014; Sanger and Shanker, 2014), and encryption keys can be obtained through indirect attacks against manufacturers of equipment with embedded keys (Scahill and Begley, 2015).

As already noted above, anybody can conduct cyber attacks: developed countries, developing countries, very small states, as well as criminal organizations. A continuing lack of concrete action to improve cyber security and to limit and control state-sponsored cyber attacks is a serious threat to the developed countries who, at present, are the least willing to take such actions.

As one human rights advocate puts the matter (Donahue, 2014): "Furthermore, by engaging in tactics that undermine digital security for individuals, for networks and for data, governments trigger and further inspire a hackers race to the bottom. Practices that undermine digital security will be learned and followed by other governments and non-state actors, and ultimately undermine security for critical infrastructure, as well as individuals users everywhere. Strengthening digital security for individual users, for data, for networks, and for critical infrastructure must be seen as the national and global security priority that it is."

[12] There are numerous restrictions at present on import, export, and even use of certain encryption methods, see for example Saper (2013).

[13] For example, the hardware might emit radio signals, or be able to receive radio signals.

Portions of critical national infrastructures are increasingly linked to and dependent on the Internet (McGuinn, 2004). If they can be disrupted by cyber attacks, that can have a significant effect on the national economy. The purpose of a national military is to protect the nation against external threats. How many military forces today are capable of protecting the civilian infrastructure against a determined cyber attack? And how many could perform effectively their traditional defense mission of using physical force if the civilian infrastructure (electrical power distribution, roads, manufacturing, etc.) is severely disrupted by a cyber attack?

4. CONCLUSIONS

Global trade and economic interdependence create incentives for nation-states to come together and agree to additional rules, or treaties, that collectively bind behavior and ensure the protection of shared resources[14]. If one considers the Internet as a microcosm of society, then its natural progression from an infant, specialized technology to the global network of networks would likely follow the path of any highly complex and interdependent community. This is to say, it is both natural and predictable that, as the Internet becomes more and more integral to the collective welfare of citizens around the world, governments will act to protect this shared resource from the abuse of malicious actors.

States should agree to cooperate to improve cyber security and to limit cyber attacks and reactions to cyber attacks. They have managed to agree to limit the types of munitions used in small arms, to limit the use of some types of mines, to limit the proliferation of nuclear weapons, and to prohibit the use of chemical weapons. A first step in the direction of cooperation to improve cyber security might be to accede to the 2012 ITRs. For sure this would not result in an immediate reduction in the number of incidents, but it would hopefully result in increased discussion and cooperation. This in turn could lead to increasing trust, thus decreasing the perceived need to engage in unilateral cyber operations. An analogy to discussions on chemical weapons and the related treaties might be appropriate. Such weapons are relatively inexpensive to develop and their use can cause severe collateral damage. Without those discussions and treaties surely there would be a greater risk of use of chemical weapons than there is at present.

Discussions on international cooperation to improve cyber security would be complex and arduous, for technical, political and social reasons (for example, improving encryption can favor both free speech and criminal activities), but every journey starts with the first step. In this case, several first steps could be taken simultaneously: the technical issues can be discussed in forums such as the ITU, the social issues in forums such as the United Nations Human Rights Council, while the political issues could be discussed at a summit to be convened by a group of willing states.

From this point of view, the results of the 2014 ITU Plenipotentiary Conference are disappointing: in order to avoid controversies and an open split within the membership, sensitive topics were not discussed in any depth (Ermert, 2014). For example, a proposal from India that included provisions that could have had the effect of improving the privacy (and hence the security) of

[14] See for example the World Trade Organization (WTO) agreements, the many treaties relating to international commerce, the treaties administred by the World Intellectual Property Organization (WIPO), the ITU treaties, etc.

domestic communications was only discussed (and dismissed) in a small group and not in the larger groups that are publicly webcast (Hill, 2014b).

Fundamentally, either we recognize that the Internet has become a global public good, and govern it accordingly (French Senate, 2015), or we continue to pretend that it is not a critical infrastructure, and we allow cyber crime and cyber attacks to flourish, which will result in medieval-style pervasive crime, violence, fear, and terror. Nobody would accept a world in which almost any criminal organization could acquire a Predator unmanned aircraft equipped with laser-guided missiles. Why should we accept the cyber-equivalent of such a situation? And if we do not wish to accept such a situation, then shouldn't we require states to cooperate to prevent its coming to pass?

The time has come to agree to cooperate to improve cyber security and to limit cyber attacks. And to focus on peaceful uses of telecommunications, which is the mission of the ITU.

ACKNOWLEDGMENT

This paper is partly based on Hill, Richard and Powers, Shawn, "Cybersecurity and spam: WCIT and the future", World Cyberspace Cooperation Summit IV, 5-6 November 2013 <http://www.hill-a.ch/EWI%20final%20rev2%20clean.pdf>. The author wishes to thank the reviewers for their helpful and constructive comments, and in particular Anna-Maria Osula for her patience and persistence.

REFERENCES

Alexander, Keith (2012), "U.S. Cyber Command Cybersecurity Legislation Position Letter", United States Cyber Command, 3 May 2012 <http://publicintelligence.net/u-s-cyber-command-cybersecurity-legislation-position-letter/>

AP (2011), "U.S. report blasts China, Russia for cyberattacks", *USA Today*, 3 November 2011 <http://usatoday30.usatoday.com/news/washington/story/2011-11-03/china-russia-cybersecurity/51065010/1>

Ball, James (2015), "Cameron wants to ban encryption – he can say goodbye to digital Britain", *The Guardian*, 13 January 2015 <http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror>

Borger, Julian (2013), "Brazilian president: US surveillance a 'breach of international law'", *The Guardian*, 24 September 2013 < http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>

Bowden, Caspar (2013), "The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights", Note for the European Parliament (2013) <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf>

Brunton, Finn (2013), *Spam: A Shadow History of the Internet*, MIT Press

CBS News (2014), "Snowden: NSA conducts industrial espionage too", *CBS News*, 26 January 2014 <http://www.cbsnews.com/news/snowden-nsa-conducts-industrial-espionage-too/>

Cerf, Vint (2012), “Can We Make the Internet Safer?” Lecture delivered at the University of Maryland’s A. James Clark School of Engineering, 7 April 2011 <http://lecture.umd.edu/detsmediasite/Play/4feab66caa824cafae6d01798b4849e51d>

Deibert, Ronald J. (2013), *Black Code: Inside the Battle for Cyberspace*, Signal (McCelland and Stewart)

Donahue, Eileen (2014), “Human Rights in the Digital Age”, *Just Security*, 23 December 2014 <http://justsecurity.org/18651/human-rights-digital-age/>

East West Institute (2012), “Building Trust in Cyberspace.” 3rd Worldwide Cybersecurity Summit in New Delhi, 2012

Eichensehr, Kristen (2014), “The Cyber-Law of Nations”, *The Georgetown Law Journal*, vol. 103, p. 317, 8 January 2014 <http://ssrn.com/abstract=2447683>

Eisenberg, Ted et. al. (1989), “The Cornell Commission: On Morris and the Worm”, *Communications of the, ACM*, June 1989, Volume 32, Number 6, p. 706

Ermert, Monika (2014), “ITU Plenipotentiary Conference: Internet Governance Diplomacy On Display”, 5 November 2014, *Intellectual Property Watch* <http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display/>

Freeman, Kevin D. (2015), “Financial Warfare Threatens America”, Global Economic Warfare, 6 March 2015 <http://globaleconomicwarfare.com/2015/03/financial-warfare-threatens-america-2/>

French Senate (2015), Proposition de resolution sur la nécessaire réforme de la gouvernance de l’Internet, Foreign Relations Committee, 22 February 2015 <http://www.senat.fr/rap/l14-102/l14-1022.html>

Gallagher, Ryan, and Greenwald, Glenn (2014), “How the NSAPlans to Infect ‘Millions’ of Comupters with Malware”, *The Intercept*, 12 March 2014 <https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/>

Gellman, Barton and Miller, Greg (2013), “‘Black budget’ summary details U.S. spy network’s successes, failures and objectives”, *The Washington Post*, 29 August 2013 <http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html>

Greenwald, Glenn (2014), “Glenn Greenwald: how the NSA tampers with US-made internet routers”, *The Guardian*, 12 May 2014 <http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden>

Haas, Richard (2010), Interview with Eric Schmidt and Jared Cohen at the Council on Foreign Relations, 29 November 2010 <https://www.youtube.com/watch?v=eJAMD5p5tQo>

Harding, Luke (2015), “Mass surveillance is a fundamental threat to human rights, says European report”, *The Guardian*, 26 January 2015 <http://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe>

Harris, Shane (2014), *@War: The Rise of the Military-Internet Complex*, Houghton Mifflin Harcourt

Headrick, Daniel R. (1991), *The Invisible Weapon: Telecommunications and international Politics 1851-1945*, Oxford University Press, p. 45

High Commissioner for Human Rights (2014), “The right to privacy in the digital age”, Report, A/HRC/27/27, 30 June 2014 <http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc>

Hill, Richard (2013), “WCIT: Failure or success, impasse or way forward?” *International Journal of Law and Information Technology*, Vol. 21 No. 3, p. 313

Hill, Richard (2013b), *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History*, Schulthess/Springer

Hill, Richard (2013c), "Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?", in Weber, R. H., Radu, R., and Chenou, J.-M. (editors) *The evolution of global Internet policy: new principles and forms of governance in the making?*, Springer/Schulthess

Hill, Richard (2014), "The Internet, its governance, and the multi-stakeholder model", *Info*, Vol. 16 No. 2, pp. 16-46

Hill, Richard (2014b), "Inside Views: What Is Happening At The ITU Plenipotentiary Conference?", *Intellectual Property Watch*, 5 November 2014 <http://www.ip-watch.org/2014/11/05/what-is-happening-at-the-itu-plenipotentiary-conference/>

Hill, Richard (2015), "The Future of Internet Governance: Dystopia, Utopia, or Realpolitik?", in Pupillo, Lorenzo (ed.), *The global Internet governance in transition*, Springer (forthcoming)

Inter-Parliamentary Union (2015), Cyber warfare: a serious threat to peace and global stability, resolution adopted by the 132ns IPU Assembly, Hanoi, 1 April 2015 <http://www.ipu.org/conf-e/132/Res-1.htm>

Internet Architecture Board (2014), IAB Statement on Internet Confidentiality, Internet Architecture Board, 14 November 2014 <https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/>

Jeffers, Dave (2013), "Security prediction for 2014: It will get worse", *PC World*, 16 December <http://www.pcworld.com/article/2080802/security-prediction-for-2014-it-will-get-worse.html>

Kaspersky Lab (2015), "Kaspersy Lab Discovers Equation Group: The Crown Creator of Cyber-Espionage, Press Release, 16 February 2015 <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-discovers-equation-group-crown-creator-cyber-espi>

Khan, Robert (2011), "The Role of Architecture in Internet Defense," in Kristin M. Lord and Travis Sharp (editors), *America's Cyber Future: Security and Prosperity in the Information Age*", Center for a New American Security, Washington, DC., June 2011

Lewis, James A. (2010), "Thresholds for cyberwar", Center for Strategic and International Studies <http://csis.org/files/publication/101001_ieee_insert.pdf>

Majority Committee Staff (2012), "Hearing on International Proposals to Regulate the Internet", *Memorandum to the Committee on Energy and Commerce*, 29 May 29 2012 <http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CT/20120531/HMTG-112-HHRG-IF16-20120531-SD001.pdf>

McCarthy, Tom (2015), "NSA director defends plan to maintain 'backdoors' into technology companies", *The Guardian*, 23 February 2015 <http://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies>

McConnell, Mike (2010), "Mike McConnell on how to win the cyber-war we're losing", *The Washington Post*, 28 February 2010 <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063>

McGuinn, Martin (2004), "Prioritizing Cyber Vulnerabilities", Final Report and Recommendations, National Infrastructure Advisory Council, 12 October 2004 <http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf>

Morozov, Evgeny (2013), "The Price of Hypocrisy", *Frankfuter Allgemeine*, 24 July 2013 <http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html>

Mueller, Milton (2012), "Threat Analysis of the WCIT: Part IV: the ITU and Cybersecurity", Internet Governance Project, 21 June 2012 <http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/>

Naughton, John (2013), “Edward Snowden’s not the story. The fate of the Internet is”, *The Guardian* 28 July 2013 <http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet>

National Security Agency (2013), “The National Security Agency: Missions, Authorities, Oversight and Partnerships”, 9 August 2013 <http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf>

Paganini, Pierluigi (2014), “NSA intercepts US-made Routers to implant surveillance”, Security Affairs, 14 May 2014 <http://securityaffairs.co/wordpress/24932/hacking/nsa-implant-surveillance-backdoor.html>

Perlroth, Nicole and Sanger, David E. (2015), “U.S. Embedded Spyware Overseas, Report Claims”, *New York Times*, 15 February 2015 <http://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html>

Poitras, Laura, Rosenbach, Marcel and Stark, Holger (2013), “Ally and Target: US Intelligence Watches Germany Closely”, *Der Spiegel*, 12 August 2013 <http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html>

Poulsen, Kevin (2015), “Surprise! America Already Has a Manhattan Project for Developing Cyber Attacks”, *Wired*, 18 February 2015 <http://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/>

Powers, Shawn, and Jablonsky, Michael (2015), *The Real Cyber War: The Political Economy of Internet Freedom*, University of Illinois Press

Powles, Julia (2015), “Charlie Hebdo and the Security State”, *Wired*, 23 January 2015 <http://www.wired.co.uk/news/archive/2015-01/23/charlie-hebdo-security-state>

Price, David (2014), “The NSA, CIA, and the Promise of Industrial Espionage”, 28 January 2014, *Counterpunch* <http://www.counterpunch.org/2014/01/28/the-nsa-cia-and-the-promise-of-industrial-espionage/>

Rand Corporation (2015), “Cyber Warfare” <http://www.rand.org/topics/cyber-warfare.html> accessed 11 February 2015

Raymond M., and Smith, G. (2013), “Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance,” Centre for International Governance Innovation, Internet Governance Papers, Paper No. 1, July 2013 <http://www.cigionline.org/sites/default/files/no1_4.pdf>

Rizo, Chris (2012), “Int’l proposals for U.N. Internet regulations draws bipartisan rebuke”, *FierceOnlineVideo*, 20 June 2012 <http://www.fierceonlinevideo.com/story/plans-un-internet-regulations-draws-bipartisan-rebuke/2012-06-20>

Rudmin, Floyd (2006), “Why Does the NSA Engage in Mass Surveillance of Americans When it is Statistically Impossible for Such Spying to Detect Terrorists?”, *CounterPunch*, 24 May 2006 <http://www.counterpunch.org/2006/05/24/why-does-the-nsa-engage-in-mass-surveillance-of-americans-when-it-s-statistically-impossible-for-such-spying-to-detect-terrorists/>

Rutkowski, Anthony (2011), “Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850”, *Info*, Vol. 13 No. 1, pp.13-31

Sanger, David (2012), “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*, 1 June 2012, p. A1

Sanger, David (2013), “U.S. Blames China’s Military Directly for Cyberattacks”, *New York Times*, 6 May 2013 <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0>

Sanger, David and Shanker, Tom (2014), “N.S.A. Devises Radio Pathway Into Computers”, *New York Times*, 13 January 2014 <http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0>

Sanger, David (2015), "President Tweaks the Rules on Data Collection", *The New York Times*, 3 February 2015 <http://www.nytimes.com/2015/02/03/world/president-tweaks-the-rules-on-data-collection.html?_r=1>

Saper, Nathan (2013), "International Cryptography Regulation and the Global Information Economy", Northwestern Journal of Technology and Intellectual Property, Fall 2013, vol. 11, p. 673 <http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/5/>

Scahill, Jeremy and Begley, Josh (2015), "The Great SIM Heist: How spies stole the keys to the encryption castle", *The Intercept*. 19 February 2015 <https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>

Schneier, Bruce (2007), "Information Security and Externalities", *Schneier on Security*, January 2007 <https://www.schneier.com/essay-150.html>

Schreier, Fred (2015) "On Cyberwarfare", DECAF Horizon 2015 Working Paper No. 7 <http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf>

Stone, Richard (2013), "A Call to Cyber Arms", *Science*, vol. 339, 1 March 2013, p. 1026

Seoul Conference on Cyberspace (2013), *Results*, <http://www.seoulcyber2013.kr/en/media/View.do?media_id=2242>

Singel, Ryan (2010), "White House Cyber Czar: 'There is no Cyberwar'", *Wired*, 4 March 2010 <http://www.wired.com/2010/03/schmidt-cyberwar/>

Talbot, D. (2006), "The Internet is broken" *MIT Technology Review*, December 2005/January 2006, p. 62 <http://www.technologyreview.com/news/405318/the-internet-is-broken/>

Tribune de Genève (2015), "De nouveax droits pour le renseignement français", *Tribune de Genève*, 17 March 2015 <http://www.tdg.ch/monde/europe/nouveaux-droits-renseignement-francais/story/14690017>

United States of America (2014), "United States Response to OHCHR Questionnaire on 'The Right to Privacy in the Digital Age'", Office of the High Commissioner for Human Rights <http://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf>

US Congress (2012), *Congressional Record*, vol. 158, no.116, Wednesday, August 1, 2012, House, pp. H5599-H5602 <http://www.gpo.gov/fdsys/pkg/CREC-2012-08-01/html/CREC-2012-08-01-pt1-PgH5599-3.htm>

WGIG (2015), *Report*, Working Group on Internet Governance, 3 August 2005 <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0>

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Visual Structures for Seeing Cyber Policy Strategies

Jennifer Stoll
Lehrstuhl für Philosophie und
Wissenschaftstheorie
Technische Universität München (TUM)
München, DE
j.stoll@tum.de

Rainhard Z. Bengez
Lehrstuhl für Philosophie und
Wissenschaftstheorie
Technische Universität München (TUM)
München, DE
bengez@web.de

Abstract: In the pursuit of cyber security for organizations, there are tens of thousands of tools, guidelines, best practices, forensics, platforms, toolkits, diagnostics, and analytics available. However according to the Verizon 2014 Data Breach Report: "after analysing 10 years of data… organizations cannot keep up with cyber crime—and the bad guys are winning." Although billions are expended worldwide on cyber security, organizations struggle with complexity, e.g., the NISTIR 7628 guidelines for cyber-physical systems are over 600 pages of text. And there is a lack of information visibility. Organizations must bridge the gap between technical cyber operations and the business/social priorities since both sides are essential for ensuring cyber security. Identifying visual structures for information synthesis could help reduce the complexity while increasing information visibility within organizations. This paper lays the foundation for investigating such visual structures by first identifying where current visual structures are succeeding or failing. To do this, we examined publicly available analyses related to three types of security issues: 1) epidemic, 2) cyber attacks on an industrial network, and 3) threat of terrorist attack. We found that existing visual structures are largely inadequate for reducing complexity and improving information visibility. However, based on our analysis, we identified a range of different visual structures, and their possible trade-offs/limitation is framing strategies for cyber policy. These structures form the basis of evolving visualization to support *information synthesis for policy actions*, which has rarely been done but is promising based on the efficacy of existing visualizations for cyber incident detection, attacks, and situation awareness.

Keywords: *cyber security policy, visualization, human-computer interaction, visual structures, organizations*

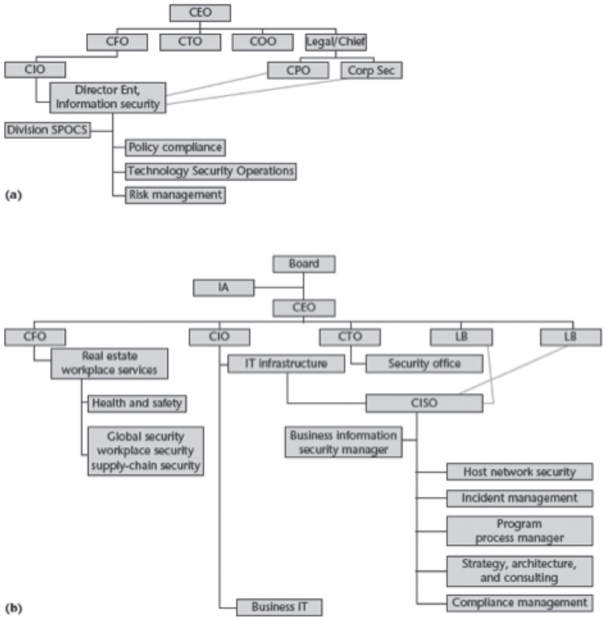
1. INTRODUCTION

A core task in making cyber policy actions is *seeing* the data that support them. In other words, decision-makers must take highly disparate data, many point of views, and synthesize them into a coherent and concise narrative that fits into a broader strategy. Yet seeing *cyber policy* remains difficult. With the growing Internet of Things, cyber policy is quickly becoming intractable for decision-makers for several reasons. One reason is the sheer complexity in terms of the volume, variety, and velocity of cyber data. To illustrate, in the Verizon 2014 Data Breach Report, over 100,000 different cyber incidents were identified in the analysis [19]. Also much of our information suffers from fragmentation. Information we need is often "trapped" in other organizations due to conflicting priorities because of privacy issues, funding issues, proprietary data and so forth. Technical concerns further exacerbate the fragmentation due to interoperability issues or inherent limitations in the design of databases and sensor systems for data collection. Additionally, much of the policy we need to see is encoded into text, because abstractions like cyber policy have not been spatialized so that they can be visualized beyond text.

Challenges for organizations: Complexity, fragmentation, interoperability issues, and lack of spatialization summarizes why cyber policy is hard to see. These four issues degrade information visibility in organizations. And the impact of these challenges is manifested in a range of organizational factors that undermine the security of organizations, while enabling challenges such as unintentional insider fraud [11]. One example is a tendency of organizational complacency towards cyber security based on erroneous perceptions of security risks. Critical information is obscured about the impact of not implementing a range of security controls to deter activities such as insider fraud or to prioritize based on areas of risk comparison. Additionally, interdependencies and the implementation of inappropriate controls result from the lack of information visibility between technical operations, managers, and non-technical staff within organizations. Basically, organizations struggle to see why certain solutions are needed are how they should fit into the broader organizational context, especially in light of other expenditures and allocation of resources.

A position paper by Johnson & Goetz [6] adds how organizational structure adds structural challenges that further hinder visibility. Figure 1 below shows two main organizational structures to highlight overlaps in responsibility and the multi-layered coordination that security tasks require. According to their study: "the security group's organizational structure is in flux and seems to undergo frequent change…It's difficult to pinpoint structural best practices because the security landscape changes so rapidly that further structural changes are likely in the coming years." [6]

FIGURE 1: "ORGANIZATIONAL STRUCTURE. (A) IN SOME ORGANIZATIONS, SECURITY MANAGEMENT REPORTS DIRECTLY TO THE CIO; (B) IN OTHERS, IT REPORTS INDIRECTLY TO THE CIO THROUGH OTHER IT EXECUTIVES." [REF]

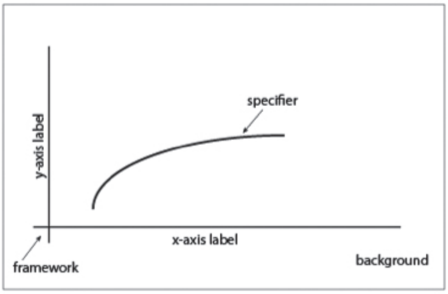


This constant shifting could indicate internal attempts by organizations to cope with the fact that security of organizations requires the cooperation and attention of all members. And the movement from area to area is a symptom of trying to find a home for security, which is a challenge because again, security needs to be part of the entire organization. The implication here is that visual structures that accommodate the multiple viewpoints present in an organization are critically needed in order to embed security within organizations and not solely IT systems.

2. VISUAL STRUCTURES

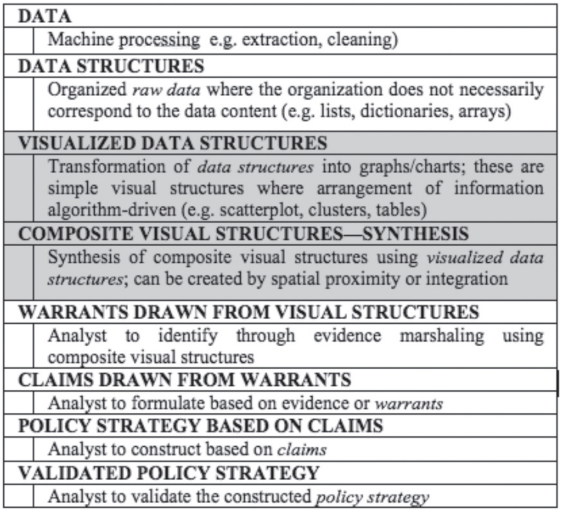
In other words, organizations must bridge the gap between technical cyber operations and the business/social priorities since both sides are essential for ensuring cyber security. Identifying visual structures for information synthesis could help reduce the complexity while increasing information visibility within organizations. This paper lays the foundation for investigating such visual structures by first identifying where current visual structures are succeeding or failing. We first conceptualize the notion of "visual structure" using the work of Kosslyn [7] who defined the components. Considered abstractly, a single visual structure such as a chart or graph according to Kosslyn, have four basic level constituent parts: 1) the background though not essential, can serve to highlight, emphasize or reinforce the information being conveyed; 2) the framework provides the mapping, the axes, or logic of the arrangement for the specifiers and labels; 3) the specifiers are elements such as lines, blocks, bars, points, and so forth, which represent the data; 4) the labels are letters, words, numbers or even pictures that help us to correctly interpret the specifiers or aspects of the framework. Figure 2 below provides a simple illustration of these parts.

FIGURE 2: VISUAL STRUCTURE COMPONENTS FOR SIMPLE GRAPH



We then extend this conceptualization to capture the structure of multiple visual structures used in conjunction, which reflects the actual core task of policy analysis where a wide-range of visuals and information are employed. We use the work of Toulmin's informal structure for building an argument, which includes the use of warrants (based on data) to marshal evidence to support claims that comprise a policy strategy or the overall "argument" [14]. Table 1 below incorporates this information structure and shows six in-between transformations of "data".

TABLE 1: CHAIN-OF-CONNECTIONS FROM RAW DATA TO POLICY STRATEGY



DATA	
	Machine processing e.g. extraction, cleaning)
DATA STRUCTURES	
	Organized *raw data* where the organization does not necessarily correspond to the data content (e.g. lists, dictionaries, arrays)
VISUALIZED DATA STRUCTURES	
	Transformation of *data structures* into graphs/charts; these are simple visual structures where arrangement of information algorithm-driven (e.g. scatterplot, clusters, tables)
COMPOSITE VISUAL STRUCTURES—SYNTHESIS	
	Synthesis of composite visual structures using *visualized data structures*; can be created by spatial proximity or integration
WARRANTS DRAWN FROM VISUAL STRUCTURES	
	Analyst to identify through evidence marshaling using composite visual structures
CLAIMS DRAWN FROM WARRANTS	
	Analyst to formulate based on evidence or *warrants*
POLICY STRATEGY BASED ON CLAIMS	
	Analyst to construct based on *claims*
VALIDATED POLICY STRATEGY	
	Analyst to validate the constructed *policy strategy*

These transformations capture where visual structures (highlighted in green) are currently being used in the process of formulating data-driven policy strategy—starting first from the raw data and culminating into the validated policy strategy. The Toulmin argument structure provides a flexible way of organizing the various information structures that could form the basis of policy. As a first step towards specifying visual structures for information synthesis in formulating policy, we identify two paths that can be taken, which are based existing visual systems used in the case studies:

- Synthesis by *proximity* where synthesis is accomplished by placing or combining individual visual structures in close spatial arrangements;
- Synthesis by *integration* where synthesis is accomplished through joining by using a common parameter to intersect the data represented by the visual structures.

An example of synthesis by proximity is the common "multi-view" visualization tools that place multiple windows of different graphs from scatterplots to timelines or clusters in close physical proximity. Often these graphs are created using the same source of data. However, they represent individual graphs only and primarily provide different views of the data. In contrast, the synthesis by integration may use the same data source, but different graphical approaches are combined into one view using common parameters. Examples of such seem to be less common but are illustrated in each of the case studies.

We use this extended conceptualization of visual structure synthesis and Kosslyn's notion of visual structure to analyze the case studies, which is presented in the following section.

3. CASE STUDIES: EPIDEMIC, CYBER ATTACKS, TERRORISM

We applied this extended notion of Kosslyn's visual structure to samples from the VAST 2011 Contest [16]. The contest involved three mini-challenges and one grand challenge where teams had to 1) characterize an epidemic spread, 2) identify cyber security issues in a corporate network, and/or 3) investigate terrorist activity in a document set. Teams were required to analyze the same raw data supplied to all teams and then using any visualization of their choice, construct a policy strategy by identifying a set of claims based on a range of evidence. The data supplied by the Challenge were synthetic, both computer and human-generated. The different datasets included: microblog messages collected from mobile GPS enabled devices, population statistics, observed weather, additional facts about geographic location, computer network architecture of the corporation, a list of security policy rules, a firewall log, an intrusion detection system log, an aggregated system logs for all hosts on network, a Nessus Network vulnerability scan report, and 4,400+ text documents. All datasets had anomalies, with only some of them being significant.

There were a total of 18 teams submitting correct solutions across the challenges. For our study, we selected eleven samples, excluding submissions with incorrect answers since our focus was to examine visualizations that support the framing analysts need to make between the raw data and the policy strategy. Our study differs from studies of argument-based systems in that we are not evaluating the soundness of an argument as in [11]. Instead, we seek to understand the relationship between the arguments formed and visualizations used for support. Our goal is not on the cognitive processes occurring inside the analyst's head, but we focus on the relationship between the visual structures and the resultant policy strategy generated from them.

Thus for each of the eleven samples, we analyzed the submissions to establish what we refer to as the chain-of-connections to go from raw data to policy strategy; and these chains identify the transformations involved in this process. After identifying a chain-of-connection from raw data to policy strategy for each submission, we compared and contrasted the Visual Data Structures and Composite Visual Structures used to generate the warrants and claims for the strategies.

A. Case #1: Epidemic

The first mini-challenge tasked teams with identifying the origin of an epidemic spread, outlining the affected area, and hypothesizing on how the epidemic is spreading. The task requires the following information to be derived from raw data: 1) three claims on origin, spread, and vector of the epidemic, and 2) the warrants or evidence to support the three claims. In the analysis, we identify a chain-of-connection for each of the three correct submissions. We refer to them as Team A, B, and C. All three teams used the same raw data provided to all teams and similar data structures: 1) thousands of microblog messages organized as a table, 2) population statistics and observed weather for specific days such as wind direction organized as a table, and 3) additional facts about the fictional city Vastopolis as well as 4) a geographic map showing landmarks.

The composite visual structure that Team A created (shown in fig. 3a) included all of the datasets. Team A correctly ascertained the origin and half of the epidemic spread by the wind to uptown Vastopolis, but failed to identify the other half spread down river.

FIGURE 3A: TEAM A'S
SPATIO-TEMPORAL MAP

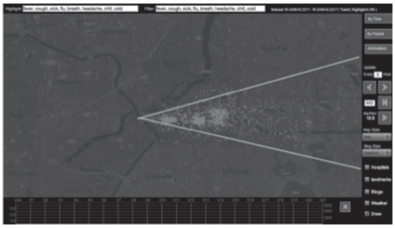
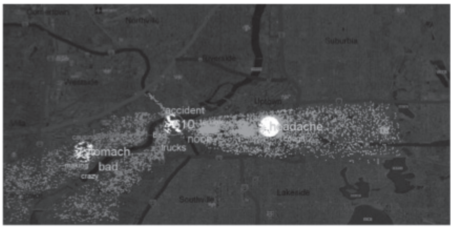


FIGURE 3B: TEAM B'S
SPATIO-TEMPORAL MAP



Team B used clusters and graph-set operations to integrate the visualized data structures along the dimension of geographic coordinates, i.e., the scatterplots and terms extracted from the microblog texts. The placement of specifiers and labels was determined solely by examining density and proximity of microblog message clusters as shown in Figure 3b. Interestingly, Team B did not attempt to incorporate the time dimension, or the weather data structure. This approach helped Team B easily identify the origin and spread of the epidemic in two primary areas, but they did not identify the vectors for spreading the disease, nor any details of timing.

Team C used all data structures to create a synthesized view and preserved views of each visualized data structure using an implied compartmentalized approach. The terms from the text extraction of the microblog message were displayed as a tag cloud cluster. While the filter terms were displayed as bars on the right. The weather and wind were displayed below the map, and a layered stack to represent the messages over time. They additionally integrated all of the visualized data structures using geographic coordinates and cardinal directions to arrange them on the map background as shown in Figures 4 and 5 below.

FIGURE 4 AND 5: TEAM C'S SPATIO-TEMPORAL MAP

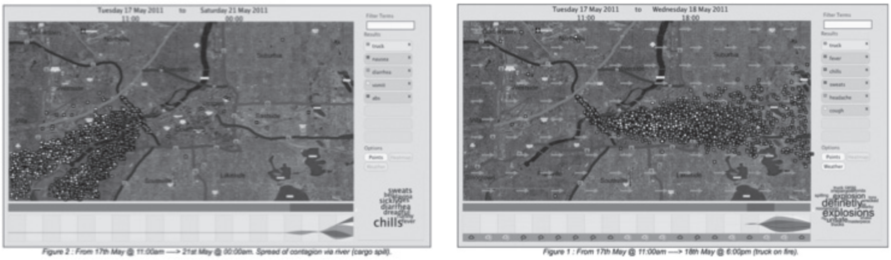
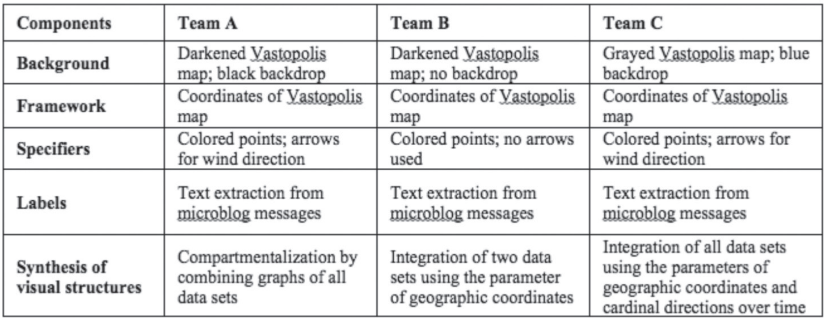


Figure 2 : From 17th May @ 11:00am —> 21st May @ 00:00am. Spread of contagion via river (cargo spill).

Figure 1 : From 17th May @ 11:00am —> 18th May @ 6:00pm (truck on fire).

In addition, interaction widgets in the implied compartments were used in the synthesized visual structure in the center. For example, selecting a specific filter term generated the geolocation as scattered points on the map; and selecting a term in the tag cloud highlighted the relevant colored dots. The background, framework, specifiers, and labels were effectively integrated into one view, including the arrows representing the wind pattern arranged on the map background. All three teams used similar visualized data structures but different composite visual structures, which are summarized in Table 2. For the background and framework, the teams used the map provided by the Challenge. For the specifiers, all three teams used colored dots to indicate the geo-location of each microblog entry. The labels utilized were also extracted from the same microblog data, indicating symptoms of illness and an unusual truck accident on fictional Highway 610 in Vastopolis. A critical difference here is that Team B did not use a visualized data structure for the weather, resulting in overlooking critical details for situation awareness such as the start date for the epidemic.

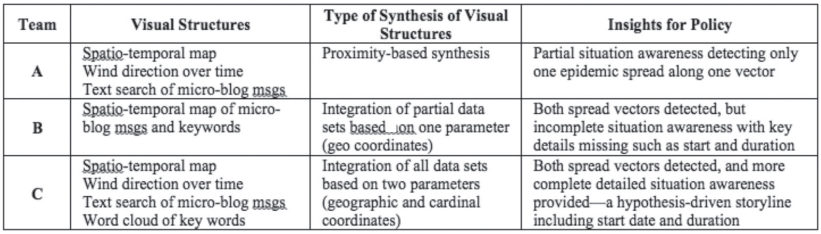
TABLE 2: VISUAL STRUCTURE COMPONENTS ACROSS TEAMS



Components	Team A	Team B	Team C
Background	Darkened Vastopolis map; black backdrop	Darkened Vastopolis map; no backdrop	Grayed Vastopolis map; blue backdrop
Framework	Coordinates of Vastopolis map	Coordinates of Vastopolis map	Coordinates of Vastopolis map
Specifiers	Colored points; arrows for wind direction	Colored points; no arrows used	Colored points; arrows for wind direction
Labels	Text extraction from microblog messages	Text extraction from microblog messages	Text extraction from microblog messages
Synthesis of visual structures	Compartmentalization by combining graphs of all data sets	Integration of two data sets using the parameter of geographic coordinates	Integration of all data sets using the parameters of geographic coordinates and cardinal directions over time

Despite using the same raw data, data structures, and similar visual structures, Team A supplied only a partially correct answer. Team B answered mostly correctly, but missed key details that would have facilitated a more complete hypothesis. However, Team C provided the most complete and correct answer that matched the posted solution for this task.

TABLE 3: CASE #1: VISUAL STRUCTURE SYNTHESIS FOR EPIDEMIC HYPOTHESIS



Team	Visual Structures	Type of Synthesis of Visual Structures	Insights for Policy
A	Spatio-temporal map Wind direction over time Text search of micro-blog msgs	Proximity-based synthesis	Partial situation awareness detecting only one epidemic spread along one vector
B	Spatio-temporal map of micro-blog msgs and keywords	Integration of partial data sets based on one parameter (geo coordinates)	Both spread vectors detected, but incomplete situation awareness with key details missing such as start and duration
C	Spatio-temporal map Wind direction over time Text search of micro-blog msgs Word cloud of key words	Integration of all data sets based on two parameters (geographic and cardinal coordinates)	Both spread vectors detected, and more complete detailed situation awareness provided—a hypothesis-driven storyline including start date and duration

As summarized in Table 3, the primary difference in the resultant policy insights generated the three teams seemed to be how the visual structures were synthesized. The integration of all data sets using multiple parameters resulted in the most complete hypothesis for the epidemic event, which would inform the situation awareness needed to take concrete policy actions for this case. This case illustrates how policy makers need to be aware that adopting different approaches for synthesizing the visual structures may result in varying degrees of hypothesis completeness.

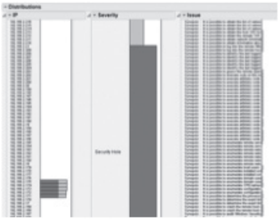
B. Case #2: Cyber Attacks on Corporate Network

For this case, we examined the submissions of five different teams using a range of visual structures to complete the task. As in the previous section, the team names are randomly assigned and do not correspond with any submission names on the VAST 2011 Challenge site. The cyber security mini-challenge task was to identify up to five security incidents of interest from the given data. The raw data supplied to and used by all teams were composite, unstructured format, and included 1) a text description of the computer network architecture, which identified priority computers, 2) a set of security policy rules, 3) firewall log data, 4) intrusion detection system log data, 5) aggregated syslogs for all the hosts on the network, and 6) a Nessus Network Vulnerability Scan Report. All teams used a range of visualized data structures and composite visual structures. In what follows, we detail the chain-of-connections for each team organized according the type of visual structure used by the team.

1) Simple Table

Team 1 imported the raw data supplied by the Challenge into a table structure and used different filter and sort functions to navigate the information as shown in Figure 6. A total of three separate tables were created for each type of log data. Using their three tables, Team 1 identified one incident of interest per table, which is described below.

FIGURE 6: TEAM 1 VISUAL STRUCTURE – SIMPLE MATRIX

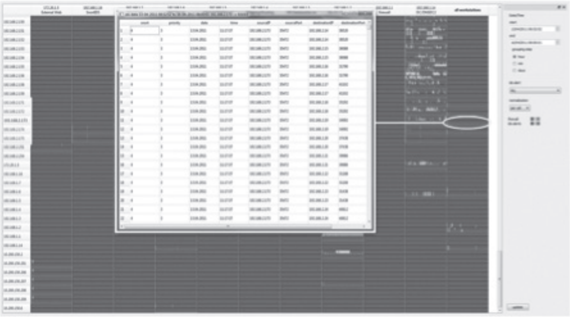


Impact of the simple table visual structure on policy strategy: These three claims with their associated warrants comprise the policy strategy of security events constructed by Team 1. Using the visual structure of a table to organize the data enabled Team 1 to easily identify incidents that generate a high frequency of the same data, e.g. message flooding. For these events, many relevant details were displayed directly, without any need to "drill in." However, infrequent, but highly important events, such as login attempts, were not found with this structure, though they were present in the data. The resultant policy strategy based on these three claims tended to focus on high-noise events and overlooked the quieter events that may be even more pernicious and difficult to detect.

2) Complex Table

Team 2 also utilized a complex table structure to organize the data by using a larger table to show the relations between each source and destination, although some machines were grouped together to reduce visual complexity. Each cell of their table contained a histogram of events that occurred between each pair of machines or groups of machines during the selected time window as shown in Figure 7. Their table also included additional sub-framework within the larger one. More specifically, analysts could select any of the histograms to drill down to a table of the raw data that it represented. They included a panel on the right to enable some basic filtering according to desired time ranges and alert types. Team 2 also used a commercially available data analysis tool (Tableau), to support some of their analysis. This was used to generate a few simple summary charts, which supported some of their warrants.

FIGURE 7: TEAM 2 VISUAL STRUCTURE – COMPLEX TABLE

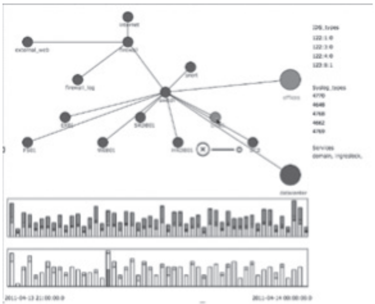


Impact of the complex table visual structure on policy strategy: The main limitation of Team 2's complex table as a visual structure is not utilizing visualization for representing overall network activity. Instead, their complex table organized the data by individual machine, and giving separate summaries of each combination of point-to-point connections. Thus, there was no chronological overview across all machines. Although summary charts generated with Tableau these summaries were not integrated with the rest of the visualization. This resulted in identifying attacks on individual machines but not when the attacks involved multiple disparate ones.

3) Graph and Histogram

As shown in figure 8, Team 3 utilized two visual data structures: a network topology graph to show locations of devices and their interrelationships, and two stacked histograms of SNORT and IDS log data.

FIGURE 8: TEAM 3 VISUAL STRUCTURE – GRAPH & STACKED HISTOGRAM



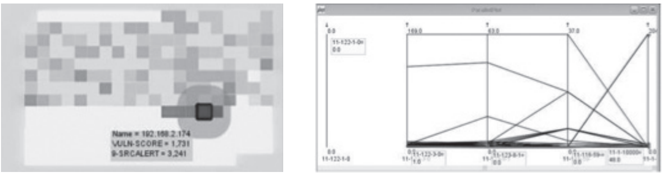
In the visual structure for the network topology, the background is implied. The framework or the logic of arrangement is dictated by how the computer network was actually set-up for the VAST 2011 Challenge data. The specifiers are the nodes and lines representing the devices on the network with corresponding labels. For the stacked histogram, the background is also implied. The framework has time on one axis and numbers of events by type on the other, with corresponding labels. The specifiers are the colored blocks of the histogram representing the total number of events by type over time with corresponding labels. Team 3 does not attempt to join the two visual structures to create a composite visual structure. Instead, Team 3 seems to use these to provide an initial overview of the data of leads for where to look at the raw data. However to find actual evidence or warrants to support their claims, they perform direct SQL queries against a database with the raw data. In other words, the chain-of-connection for Team 3 effectively bypasses the "visual data structure" and "composite visual structure" steps of the chain. This indicates that members of Team 3 relied primarily on their domain knowledge to navigate a way through the raw data.

Impact of the graph and stacked histogram visual structure on policy strategy: The visual structure of the network topology combined with the views of the stacked histogram, enabled team 3 to see some initial relevant information for both the whole network and the significant entities (machines, traffic, and events) over time. As their claims collectively demonstrate, this particular visual structure supports uncovering insights showing the impact of a machine on a network. However, one limitation is the difficulty seeing machine-specific issues within subnets: the visual structure obscured the presence of individual machines within the "offices" and "datacenter" subnets in both the topology as well as the histogram. This visualization served primarily as an overview and a starting point for constructing SQL queries. Thus these queries, rather than the visual structures, were then used in identifying 4 different attacks. Such visualization could be initially useful for domain experts, but less so for non-expert policy makers.

4) Simple Heat Map & Parallel Coordinate Plot

As indicated by figure 9a&b, Team 4 utilized two visual data structures: a simple heat map that presented traffic and alerts per machine, and a parallel coordinate plot that showed IDS log data on a per hourly basis. The granularity of the heat map was per machine, with a single block of the map representing one device on the network. The visual structure framework organizes IDS log data using time (per hour), source and destination nodes as the axes.

FIGURE 9A & 9B: TEAM 4 VISUAL STRUCTURE – SIMPLE HEAT MAP AND PARALLEL COORDINATE PLOT

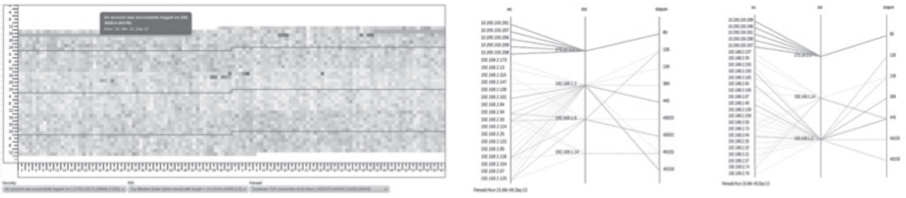


Impact of the heat map and parallel coordinate plot visual structure on policy strategy: The visual structure of a simple heat map combined with a parallel coordinate plot enabled Team 4 to easily see issues occurring on a per-machine and per-hour basis. This visualization provided an effective summary, but seemed to obscure infrequent but highly important events, such as the RDP login to the webserver. This visual structure did not easily reveal events that overlapped hours or machines, due to compartmentalization of the time slices to per-hour sections, and the relations between different machines were often not clear. This may have contributed to many of their claims lacking detail and specificity with regard to situation awareness.

5) Complex Heat Map & Parallel Coord. Plot

Team 5 also used two visual data structures: a complex heat map and a parallel coordinate plot, both at finer granularities as shown in figure 10a & b below.

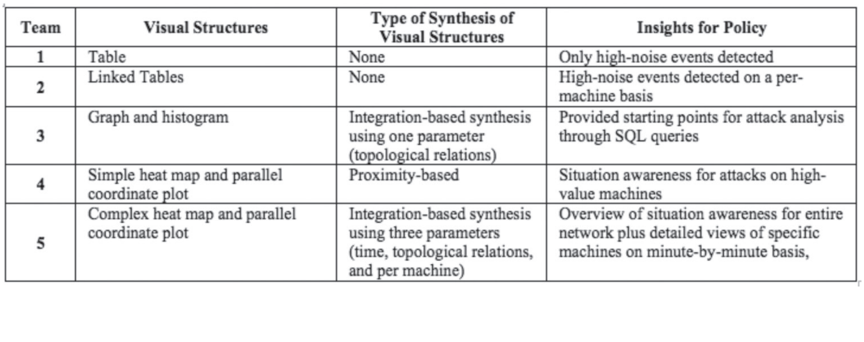
FIGURE 10A & 10B: TEAM 5 VISUAL STRUCTURE – COMPLEX HEAT MAP AND PARALLEL COORDINATE PLOT



For the complex heat map, the background was a bounded outline. The framework used time on the y-axis and event types on the x-axis, with corresponding labels. The specifiers were colored blocks for the entire network that changed colors depending on network traffic levels per event type per minute of each hour, with corresponding labels. For the parallel coordinate plot, the background is implied. The framework uses parallel axes of addresses of source (src) nodes on the network, destination nodes (dst), and the destination port (dstport). The specifiers are lines representing traffic from nodes to ports, with corresponding labels (e.g., src: 192.168.2.25, dst: 192.168.1.14, dstport: 445).

Impact of visual structure on policy strategy: Team 5's visualizations were particularly effective for showing time relationships between various events, which allowed causal sequences of events to be determined. This is often extremely important, such as identifying events where there were user logins to several machines immediately before they began scanning the rest of the network. The visualizations used by the other teams indicated the presence of scans, but were not able to convey important additional details such as these logins related to the scans. Team 5's complex heat map organized by time and machine remains a consistent visual structure throughout, providing continuous context, but also many useful filters to highlight various categories of events before relying on the parallel coordinates chart for still more additional details. Their visual structure enabled seeing issues related to the entire network using a fine-grained minute-by-minute representation, and well as going into the specific related data structure to identify related critical information.

TABLE 4: CASE #2: VISUAL STRUCTURE SYNTHESIS FOR CYBER ATTACK ANALYSIS



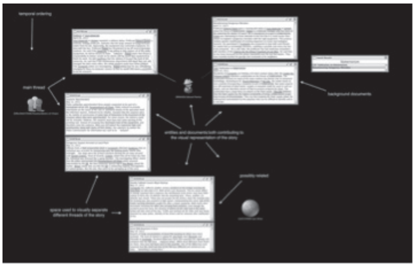
Team	Visual Structures	Type of Synthesis of Visual Structures	Insights for Policy
1	Table	None	Only high-noise events detected
2	Linked Tables	None	High-noise events detected on a per-machine basis
3	Graph and histogram	Integration-based synthesis using one parameter (topological relations)	Provided starting points for attack analysis through SQL queries
4	Simple heat map and parallel coordinate plot	Proximity-based	Situation awareness for attacks on high-value machines
5	Complex heat map and parallel coordinate plot	Integration-based synthesis using three parameters (time, topological relations, and per machine)	Overview of situation awareness for entire network plus detailed views of specific machines on minute-by-minute basis,

As summarized in Table 4, the different visual structures used resulted in the detection of different classes of attacks from high-noise, low-noise, machine-specific, and so forth. Also, the synthesis of the visual structures impacted the range of attacks that were detected using visualizations. Team 5, which integrated the visual structures using the most parameters, was able to provide both high-level and fine-grained analysis of cyber events in the network. This case again illustrates the need to consider how the use of proximity-based synthesis of visual structure results in significantly different situation awareness than using integration-based synthesis. Also, increasing the number of parameters for integration seems to result in more complete situation awareness.

C. Case #3: Terrorist Plot

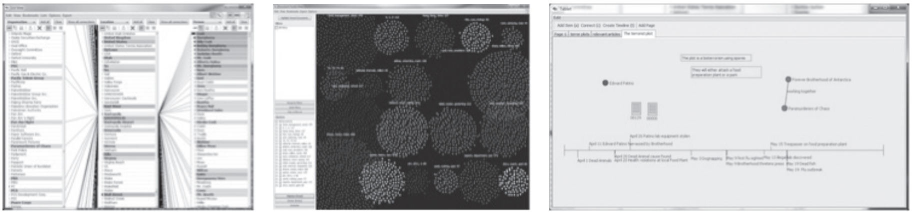
Teams were tasked to analyze a corpus of documents (n=4,474). Each team created different diagrams from the raw document data to support their policy strategy construction of possible terrorist activity. The goal was to identify all documents relevant to an actual terrorist plot (13 total). For their visual data structure, Team A created a node-link diagram that interconnected related clusters of documents as shown in Figure 11 below.

FIGURE 11: TEAM A VISUAL STRUCTURE – NODE-LINK DIAGRAM OF DOCUMENT CLUSTERS


temporal ordering
main thread
background documents
entities and documents both contributing to the visual representation of the story
possibly related
space used to visually separate different threads of the story

The document clusters were created using entity extraction and a vector-space model, to build graphs of both sentence-based and document-based co-occurrence, as well as document-neighbor discovery. Based on the extractions, the documents were then examined for items of interest. Key entities and phrases were temporally arranged based on related themes, entities and events for further analysis. Using a visualize structure which synthesized data using a compartmentalized approach, Team A correctly identified five out of thirteen documents needed for constructing a reliable policy strategy.

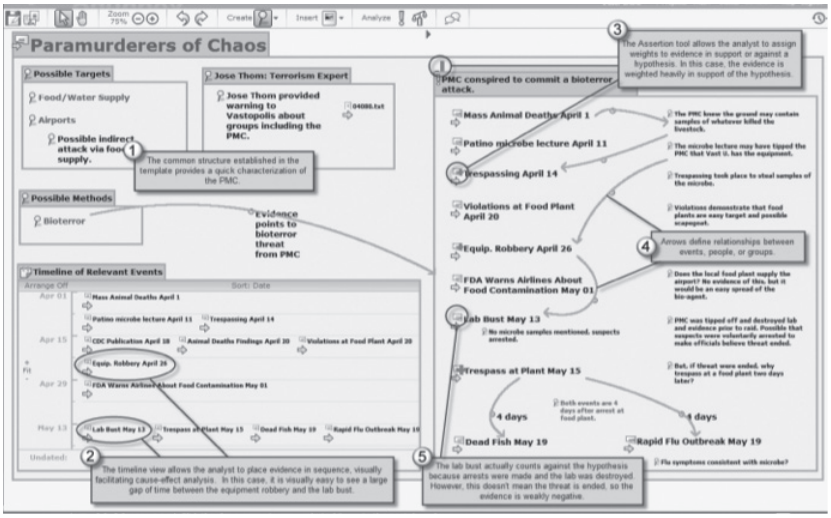
FIGURE 12A,B & 13: TEAM B VISUAL STRUCTURE – 3 OF 5 VIEWS



As partially illustrated in figs. 12a,b and 13, Team B created a total of five visual data structures from the raw document data after first extraction and manually cleaning: 1) a list view, 2) cluster view, 3) document view, 4) calendar view, and 5) timeline view. The list view grouped related entities, while the cluster view grouped related documents. The document view enabled detailed exploration of related documents using a tag cloud to navigate the document set. The calendar view ordered documents identified as suspicious according the dates associated with the documents, while the timeline ordered the notes from the analysis according to relevance and order of occurrence. Using a hybrid-synthesis of compartmentalized visual structures and simple, integrated structures based on the time parameter, Team B correctly identified 11 of 13 documents needed for constructing their policy strategy. However, they also included in the solution one false lead and three isolated incidents unrelated to the imminent threat.

In contrast, Team C used indented lists inside an integrated visual structure that laid out multiple timelines within different hypothesis-driven story lines, which resulted in a nested visual framework approach. Their synthesis of visual structure enabled them to organize the specifiers and labels of indented lists representing the raw data. They preprocessed the data using both custom and standard dimensions for extracting and clustering documents of interest. They manually reviewed these documents, and manually extracted information of interest to create an initial timeline view.

FIGURE 14: TEAM C VISUAL STRUCTURE SYNTHESIS – EXAMPLE NESTED FRAMEWORK


Zoom 75%
Create
Insert
Analyze
Paramurderers of Chaos
Possible Targets
Food/Water Supply
Airports
Possible indirect attack via food supply.
Jose Thom: Terrorism Expert
Jose Thom provided warning to Vastopolis about groups including the PMC.
04086.txt
Possible Methods
Bioterror
Evidence points to bioterror threat from PMC
Timeline of Relevant Events
Arrange Off
Sort: Date
Apr 01
Mass Animal Deaths April 1
Patino microbe lecture April 11
Trespassing April 14
Apr 15
CDC Publication April 18
Animal Deaths Findings April 20
Violations at Food Plant April 20
Equip. Robbery April 26
Apr 29
FDA Warns Airlines About Food Contamination May 01
May 13
Lab Bust May 13
Trespass at Plant May 15
Dead Fish May 19
Rapid Flu Outbreak May 19
Undated:
Fit
PMC conspired to commit a bioterror attack.
Mass Animal Deaths April 1
Patino microbe lecture April 11
Trespassing April 14
Violations at Food Plant April 20
Equip. Robbery April 26
FDA Warns Airlines About Food Contamination May 01
Lab Bust May 13
No microbe samples mentioned, suspects arrested.
Trespass at Plant May 15
4 days
Both events are 4 days after arrest at food plant.
4 days
Dead Fish May 19
Rapid Flu Outbreak May 19
The PMC knew the ground may contain samples of whatever killed the livestock.
The microbe lecture may have tipped the PMC that Vast U. has the equipment.
Trespassing took place to steal samples of the microbe.
Violations demonstrate that food plants are easy target and possible scapegoat.
Does the local food plant supply the airport? No evidence of this, but it would be an easy spread of the bio-agent.
PMC was tipped off and destroyed lab and evidence prior to raid. Possible that suspects were voluntarily arrested to make officials believe threat ended.
But, if threat were ended, why trespass at a food plant two days later?
Flu symptoms consistent with microbe?
1
2
3
4
5

1 The common structure established in the template provides a quick characterization of the PMC.

2 The timeline view allows the analyst to place evidence in sequence, visually facilitating cause-effect analysis. In this case, it is visually easy to see a large gap of time between the equipment robbery and the lab bust.

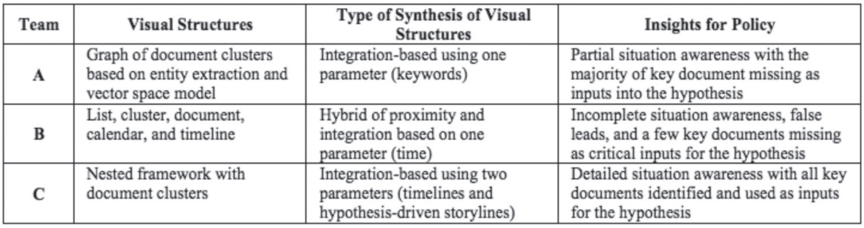
3 The Assertion tool allows the analyst to assign weights to evidence in support or against a hypothesis. In this case, the evidence is weighted heavily in support of the hypothesis.

4 Arrows define relationships between events, people, or groups.

5 The lab bust actually counts against the hypothesis because arrests were made and the lab was destroyed. However, this doesn't mean the threat is ended, so the evidence is weakly negative.

Separate timelines were then created for several competing hypotheses coupled with related documents. One of the hypotheses of interest was selected for further development. The selected hypothesis was used as the framework to integrate timelines, warrants, sub-claims that supported the hypothesis, i.e., associated extractions and clusters from the processed raw data were tied to specific hypotheses, which was organized according to entities. Figure 14 shows such a synthesis for the entity "Paramurderers of Chaos." In other words, Team C synthesized the visual structure using entities as the primary parameter for integration, and timelines within hypothesis-driven storylines components (targets, expert perspective, methods, warrants) as additional sub-parameters for data integration. Team C correctly identified all thirteen documents needed for constructing their policy strategy.

TABLE 5: CASE #3: VISUAL STRUCTURE SYNTHESIS FOR POSSIBLE TERROR ATTACK



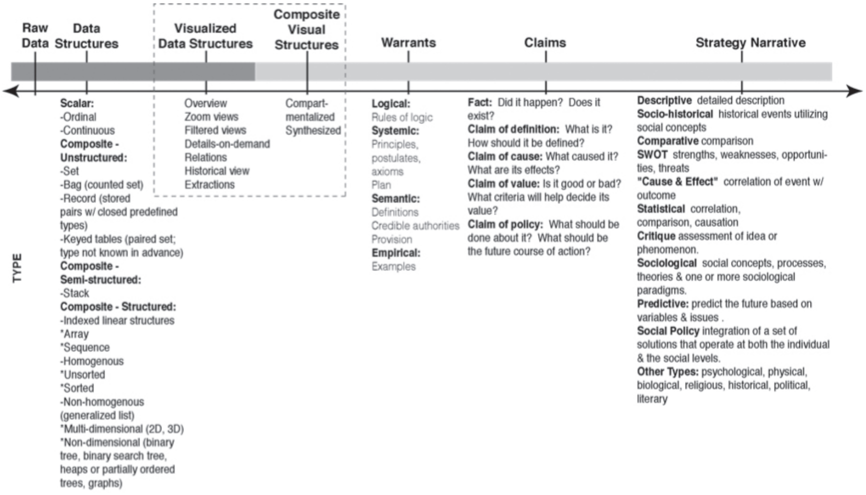
Team	Visual Structures	Type of Synthesis of Visual Structures	Insights for Policy
A	Graph of document clusters based on entity extraction and vector space model	Integration-based using one parameter (keywords)	Partial situation awareness with the majority of key document missing as inputs into the hypothesis
B	List, cluster, document, calendar, and timeline	Hybrid of proximity and integration based on one parameter (time)	Incomplete situation awareness, false leads, and a few key documents missing as critical inputs for the hypothesis
C	Nested framework with document clusters	Integration-based using two parameters (timelines and hypothesis-driven storylines)	Detailed situation awareness with all key documents identified and used as inputs for the hypothesis

4. IMPLICATIONS FOR CYBER POLICY INSIGHT

These case studies demonstrate a gap in our understanding of composite visual data structures, and how their synthesis can drastically reduces or illuminates the direction of policy strategy. As illustrated by the first case study, the *cyber policy* strategies we are able to see depends on how visual structures are used to synthesize data. E.g., for Case 1 Epidemic, the team used an *integrated* approach rather than a proximity approach, and was thus able to compile a more complete situation awareness to inform action. In Case 2 Cyber Attacks, the team using the *most parameters* for synthesizing the visual structures was able to identify the broadest range of attacks on the corporate network. And in Case 3 Terrorist Plot, the team used a nested framework to support a *narrative-based integration* parameter and was able to construct the most reliable hypothesis to inform situation awareness. The key implication for cyber policy is that these case studies point toward a critical need to further investigate how visual structures are synthesized and how they inform policy action.

We offer the following spectrum of information structures as a starting point in figure 15 below. Based on the Toulmin argument structure, this spectrum represents an initial chain-of-connections from data to policy strategy/narrative.

FIGURE 15: CHAIN-OF-CONNECTIONS FROM RAW DATA TO NARRATIVE


Raw Data
Data Structures
Visualized Data Structures
Composite Visual Structures
Warrants
Claims
Strategy Narrative
TYPE
Scalar:
-Ordinal
-Continuous
Composite - Unstructured:
-Set
-Bag (counted set)
-Record (stored pairs w/ closed predefined types)
-Keyed tables (paired set; type not known in advance)
Composite - Semi-structured:
-Stack
Composite - Structured:
-Indexed linear structures
*Array
*Sequence
-Homogenous
*Unsorted
*Sorted
-Non-homogenous (generalized list)
*Multi-dimensional (2D, 3D)
*Non-dimensional (binary tree, binary search tree, heaps or partially ordered trees, graphs)
Overview
Zoom views
Filtered views
Details-on-demand
Relations
Historical view
Extractions
Compart-mentalized
Synthesized
Logical:
Rules of logic
Systemic:
Principles, postulates, axioms
Plan
Semantic:
Definitions
Credible authorities
Provision
Empirical:
Examples
Fact: Did it happen? Does it exist?
Claim of definition: What is it? How should it be defined?
Claim of cause: What caused it? What are its effects?
Claim of value: Is it good or bad? What criteria will help decide its value?
Claim of policy: What should be done about it? What should be the future course of action?
Descriptive detailed description
Socio-historical historical events utilizing social concepts
Comparative comparison
SWOT strengths, weaknesses, opportuni-ties, threats
"Cause & Effect" correlation of event w/ outcome
Statistical correlation, comparison, causation
Critique assessment of idea or phenomenon.
Sociological social concepts, processes, theories & one or more sociological paradigms.
Predictive: predict the future based on variables & issues .
Social Policy integration of a set of solutions that operate at both the individual & the social levels.
Other Types: psychological, physical, biological, religious, historical, political, literary

This chain-of-connection begins with "raw data" and enumerated "data structures" [1] because they form the basis of policy actions. Acting as a link, "visual structures"—both individual and composite—create a bridge between data and the "warrants" and "claims" that comprise "policy strategy/narrative". The dashed box outlining both types of visual structures highlight their importance in shaping our understanding of situation awareness for policy action. Currently, most cyber policy is informed by visualized data structures rather than composite visual structures that support higher-order information structures enumerated along the blue bar in Figure 15.

The implications for cyber policy are several. First, there is a critical to investigate how visual structures can help synthesize the information needed to inform policy decisions, which tend to fall into three categories: standard, irregular, and emergency. Decisions that are "Standard" are routine decisions where procedures are well-established, and historical data is likely available. In contrast, "Irregular" decisions that are outside the routine, but not urgent, while decisions that are "Emergency" are both irregular and time-sensitive. Identifying visual structures could help reduce the complexity of information for each of these three different types of policy decisions. That is, these patterns would facilitate both short and long-term analytics of policy actions based on data as well as provide alternate perspectives in understanding future decision-making. In other words, these visual patterns could also help streamline the information flow process in organizations by connecting policy strategy from the past with future decisions to be made.

However, there are caveats in pursuing these visual structures for information synthesis, which is illustrated by a case study for the Federal Chancellery of a European country [13]. The first caveat is that while visualization of information is important, it is only useful if it is integrated in an information flow process that is part of the decision-making. The second caveat is that simplicity in the visualization supported decision-making much more than complex ones.

Organizations need an innovative approach that 1) efficiently conveys policy prescriptions and 2) provides mechanisms for synthesizing these prescriptions with recommendations for policy actions in organizations [3]. One approach, which we will investigate in future work, is to develop patterns of cyber policy[1] in organizations, which can be visualized for the three different categories of decisions: standard, irregular, and emergency. Identifying and developing policy patterns would enable policy to be efficiently conveyed and provides a framework for synthesizing policy information in organizations.

A number of different patterns for cyber security have been developed for attacks, forensics, vulnerabilities, and user behavior. However, patterns of visual structures for cyber policy in organizations have not been the focus of cyber security research beyond complex text-based prescriptions. Visual policy patterns for organizations would be novel, but rely on the proven success of using visualization for cyber security. These patterns of visual structures could help organizations move beyond incremental security and towards innovative management of policy for issues like unintentional insider threats.

In future work, our plan is to develop a complementary framework to Kosslyn's visual structure to analyze the information content conveyed by visual structures. Having this dual-framework of visual structure and information content could enable policy makers to better assess the data foundation of their strategy and to consider alternate perspectives offered by differently structured visualizations.

REFERENCES

[1] Dale, N., and Walker, H. A classification of data types. Computer Science Education 3.3 (1992): 223-232.

[2] Harvey, M., Long, D., Reinhard, K. Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security. Power and Energy Conference at Illinois (PECI), 2014.

[3] Herath, T., Rao, H.R. Encouraging Information Security Behaviors in Organizations: Role of penalties and perceived effectiveness. Decision Support Systems 47 (2009) 154-165.

[4] Hossain, M. et al. 2012. Storytelling in Entity Networks to Support Intelligence Analysts. Proceedings of the ACM Conference on KDD'12, Beijing, China.

[5] Isenberg, T., Isenberg, P., Chen, J., Sedlmair, M., Möller, T. 2013. A Systematic Review on the Practice of Evaluating Visualization. IEEE TVCG, Oct. 2013.

[6] Johnson, Eric; Goetz, Eric. 2007. Embedding Information Security into the Organization. IEEE Security & Privacy, May/June 2007.

[7] Kosslyn, S. M., 1989. Understanding Charts and Graphs." Applied Cognitive Psychology, Vol. 3, 185-225.

[8] Lam, H., Bertini, E., Isenberg, P., Plaisant, C., Carpendale, S. Empirical Studies in Information Visualization: Seven Scenarios. 2012. IEEE TVCG, 18(9):1520-1536, Sept. 2012.

[9] Lowrance, J. D., Harrison, I. W. & Rodriguez, Andres C. 2000. Structured Argumentation for Analysis. Proc. of 12th Int'l Conf. on Systems Research, Informatics, and Cybernetics, Baden-Baden, Germany, pp. 47-57.

[10] North, C. 2006. Toward measuring visualization insight. IEEE CGA, 26(3):6-9, May/June 2006.

[11] Reed, C. and Rowe, G. 2004. Araucaria: Software for argument analysis, diagramming and representation. International Journal on Artificial Intelligence Tools 13.04: 961-979.

[12] Samonas, S. Originally presented at 12th Annual Security Conference, Keynote Lecture. 11 April 2013, Las Vegas, Nevada. This version available at: http://eprints.lse.ac.uk/50344/

[1] A simple example of a policy pattern is password generation required four different character sets. A more complex example is the "Baseline Security" provided by the German government or "Common Criteria", an international standard for cyber security.

[13] Stoll, J., Siemssen, J., Bengez, R. Visualization, Insider Cyber Threats & Legal Informatics. To be published in the Proceedings of the ACM Austria: Internationales Rechtsinformatik Symposion (IRIS 2015).

[14] Toulmin, S. E. (2003). The uses of argument. Cambridge University Press.

[15] Visual Analytics Science & Technology, 2011. www.visualanalytics.com

[16] Wickham, H., Cook, D., Hofmann, H., Buja, A. 2010. Graphical Inference for Information Visualization. IEEE TVCG, Vol. 16, No. 6.

[17] Yi, JS., Kang, Y., Stasko, J., Jacko, J. 2008. Understanding and Characterizing Insights: How do People Gain Insights Using Information Visualization? BELIV, Florence, Italy.

[18] Ziemkiewicz, C., Gomez, S., Laidlaw, D. 2012. "Analysis Within and Between Graphs: Observed User Strategies in Immunobiology Visualization." CHI'12, Austin, TX.

[19] Verizon. 2014. Data Breach Investigations Report. Accessed: www.verizonenterprise.com/DBIR/2014

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Strategic Anti-Access/Area Denial in Cyberspace

Alison Lawlor Russell, Ph.D.
Department of Political Science
Merrimack College
North Andover, MA USA
russella@merrimack.edu

Abstract: This paper investigates how anti-access and area denial (A2/AD) operations can be conducted to deny actors access to cyberspace. It examines multiple facets of cyberspace to identify the potential vulnerabilities within the system that could be exploited. This project will also touch upon the policy implications of strategic cyber A2/AD for national security, particularly as they relate to deterrence strategy, coercion, and interstate conflict.

The question of deterrence is particularly important. Given the extensive reliance of modern states and societies on cyberspace, the ability to deny access to cyberspace would threaten the economy, security, and stability of a state. A credible threat of this nature may be sufficient to deter armed conflict or compel a more favorable course of action. Thus, strategic A2/AD in cyberspace may create new options and tools for international relations.

This paper will address strategic A2/AD with regards to the physical aspects of cyberspace (i.e., cables, satellites). It will assess the strengths and potential vulnerabilities of the physical attributes (the architecture) of cyberspace, as they relate to potential A2/AD operations. It will also address the relevant policy and strategy implications of strategic cyber A2/AD for states, including how this may affects the development of cyber security strategy, critical infrastructure protection, and private sector cooperation. The paper will offer conclusions and recommendations to policymakers and scholars.

Keywords: *infrastructure, anti-access/area denial, A2/AD, strategy, deterrence, conflict*

1. INTRODUCTION

The Information Age of the twenty-first century is distinguished by the proliferation of networks of power that transmit information in a variety of forms and have the effect of defining and decentralizing power relationships. The instantaneous transmission of information through vast geographic space has made our current global economic system possible, as it has the operations of modern governments, militaries, and social organizations. Their capabilities hinge on the accessibility of cyberspace to all participants. To be absent from these networks of information is to be absent from power.[1]

Cyberspace is the modern communications network that underpins global information exchange and services. It is ubiquitous, complex, and much bigger than the internet alone. It underpins the global economic order and is essential to all elements of state power, from military operations to electricity to basic communications. Old networks, such as plain old telephone systems, have been integrated into the newer and more efficient networks of cyberspace. Cyberspace is so ubiquitous that strategic connectivity is rarely questioned.

Nevertheless, connectivity to cyberspace should not be taken for granted, especially by states. Cyberspace is a man-made network to which a state can be connected and disconnected, sometimes against its will. Cyber blockades can occur and states can be denied access to cyberspace[2]. The experience of North Korea in December 2014 illustrated just how quickly and completely a state can be denied access to cyberspace. For nine and a half hours on December 22nd, North Korea suffered a total outage of internet connectivity. At the time of writing, the cause the incident were still being investigated, but the event was consistent with a cyber attack, and it came just days after the U.S. Federal Bureau of Investigation said that North Korea was responsible for a major cyber attack on Sony Pictures. However, experts cautioned that the event could also be attributed to other causes, such as power problems.[3]

Deliberate actions to deny a state access to cyberspace and/or diminish its capacity to operate freely therein may be considered anti-access and area denial operations. The modern understanding of anti-access and area denial operations (or A2/AD operations, as this article will refer to it) specifically means to deny an adversary the ability to bring its operational capabilities into the contested region or to prevent the attacker from operating freely within the region and maximizing its capabilities.[4]

This definition of A2/AD strategy evolved from assessments of anti-access warfare strategies in other domains, that is, on land, at sea, and in the air. The United States Department of Defense has designated cyberspace the “fifth domain” for defensive operations and warfighting, thus it is appropriate and prudent to investigate the extension of strategies, such as A2/AD from the other domains to cyberspace.[5]

The goal of this paper is to examine how A2/AD can occur at the physical layer of cyberspace and understand some of the implications of this for policy and strategy[6]. This article will begin with

[1] Manuel Castells, *Communication Power* (New York: Oxford University Press, 2009).

[2] Alison Lawlor Russell, *Cyber Blockades* (Washington DC: Georgetown University Press, 2014).

[3] Chloe Albanesius, “Internet in North Korea Offline after Apparent Attack,” PC Magazine, http://www.pcmag.com/article2/0,2817,2474065,00.asp.

[4] Sam J. Tangredi, *Anti-Access Warfare : Countering A2/Ad Strategies* (Annapolis, Maryland: Naval Institute Press, 2013), 1-2.

[5] Cyberspace differs from the other domains in three important ways. Firstly, the other domains would exist without human action. Cyberspace was created by humans and will cease to exist and function without continued human interaction and upkeep. Secondly, cyberspace traverses the other domains. Fiber optic cables run along the sea floor, satellites transmit information, wireless signals fly through the air. The other domains touch, but do not rely on each other in the same way that cyberspace relies on the other domains. Thirdly, the topography of cyberspace is constantly changing and being modified by human interaction. As the terrain is constantly changing, it is especially difficult to protect and defend against attacks.

[6] This article is part of a broader research project to examine A2/AD at all layers cyberspace. To meet CYCON publication requirements, this article will focus solely on the physical layer of cyberspace.

an overview of anti-access warfare and A2/AD strategies. Next, it will examine the elements of the physical layer of cyberspace, specifically cables, satellites, and the electromagnetic spectrum and discuss their potential vulnerabilities to A2/AD operations. Lastly, the article will conclude with a discussion about the implications of this for cyber security and strategy for policy makers and scholars.

2. ANTI-ACCESS WARFARE AND A2/AD

2.1 Anti-Access Warfare

Written records of anti-access warfare strategies date back 480 B.C., when the independent city-states of Greece were menaced by the Persian emperor Xerxes and the largest armed force ever assembled at that time[7]. According to the historian Herodotus, Xerxes' forces numbered 1.7 million troops, and 1,327 warships (although the number of troops was, in all likelihood, much smaller; the larger number may have included warriors as well as camp followers). In contrast, the Greek city-states had only a few thousand defenders each and they had rarely before been united.[8]

The weaker Greek city-states were able to defeat Xerxes and his great army by pursuing a strategy of anti-access. By preventing the necessary supply ships from reaching the soldiers ashore, they turned Xerxes strength into a weakness; his army was too big to live off the land and could not survive without shipments of grain, which could only be brought by sea. The power of the anti-access strategy is that it allowed the weaker force to prevent the stronger force from bringing its resources to bear in the theater of operations; it neutralized the superior force and then waited for time, attrition, and/or extrinsic events to shake the determination of the attacker.[9]

A2/AD operations include a variety of military activities that can occur on land, in the air, at sea, and in space. Traditionally, A2/AD activities have been designed to establish and maintain control of the battlespace—an objective of any military force. The goal is to deny the adversary the ability to enter the area and maneuver freely within the battlespace. Anti-access and area denial are different, but related concepts that offer a nuanced approach to deny the adversary the ability to operate within a contested zone.

Anti-access traditionally refers to the ability to cordon off an area and control entry to it, thus to effectively deny the adversary entry to the contested area. Area denial refers to the ability to diminish, degrade, or destroy the adversary's freedom of action within the contested area. In short, A2 affects movement to a theater, while AD affects movement *within* a theater.

From the U.S. perspective, A2/AD is a contingency for which it must plan for and against. In some cases, the U.S. military may seek to employ A2/AD strategies against an adversary, while in other cases, an adversary may try to use an A2/AD strategy against the U.S. military. Within the U.S. military and policy community, A2/AD is also commonly associated with the "AirSea

[7] For an excellent historical analysis of anti-access warfare, see Tangredi, *Anti-Access Warfare : Countering A2/Ad Strategies*.

[8] Ibid., 7-8.

[9] Ibid., 8-15.

Battle Concept" and other joint operations, it is also applicable to the cyber domain, where access is a necessary precondition to being able to operate from any distance.

2.2 Anti-Access/Area Denial (A2/AD) Operations in Cyberspace

The concept of A2/AD as it pertains to cyberspace is a relatively recent and evolving concept in warfare. Most of the extant literature about anti-access warfare or anti-access and area denial strategies focuses on what has been done historically at sea, in the air, and on land, and what is being discussed now regarding U.S. military planning for future threats, specifically those that might emanate from Asia[10]. Information and communications has long been considered as a key to victory or defeat in conflict, whether it was Sun Tzu's emphasis on intelligence gathering and deception, or more recent decision-making theories such as Boyd's OODA loop theory. A2/AD in cyberspace does not seek to manipulate the information itself, but rather to disrupt and prevent the flow of information.

The capability to conduct A2/AD in cyberspace, or "cyber A2/AD," exists on two levels. At the tactical level, cyberspace can be used as an avenue for conducting cyber attacks that will result in A2/AD of other domains. For example, sophisticated cyber attacks may be designed to destroy specific satellite imagery capabilities, missile targeting, or even navigational equipment to facilitate A2/AD operations at sea or in the air.[11] This level of cyber A2/AD is commonly discussed and relatively well-known by operational planners and cyber tactical teams.

At the strategic level, cyber A2/AD receives very little attention and is relatively under-examined by scholars and policy makers. This strategic cyber A2/AD is the target of this research paper. Strategic cyber A2/AD is defined here as the ability to gain control of the network or infrastructure of cyberspace and manipulate it in such a way as to deny a state the ability to use cyberspace *in any capacity*. Unlike tactical cyber A2/AD, it does not target the functionality of specific weapons or information systems that are connected to cyberspace, but rather targets states' access to the grid itself.[12]

A2/AD in cyberspace is of significant and increasing concern for US national security. In the Joint Operation Access Concept of 2012, U.S. Department of Defense (DoD) identified three trends that directly led to the increase of A2/AD capabilities around the world in recent years. One of these trends is the "*emergence of space and cyberspace as increasingly important and contested domains*" (emphasis added) as a factor affecting the rise of A2/AD threats. In addition to proliferation of advanced technologies and changing US defensive posture, the proliferation

[10] There is a dearth of scholarly literature on anti-access warfare, with the notable exception of Sam J. Tangredi's book *Anti-Access Warfare*, while the media and government reports on the subject tend to focus on the specifics of current military planning. Discussions of anti-access warfare and cyberspace in any of the literature are rare and usually quite limited.

[11] Harry Kazianis, "The Real Anti-Access Story: Cyber " *Flashpoints: Diplomacy by Other Means* (2013), http://thediplomat.com/flashpoints-blog/2013/05/15/the-real-anti-access-story-cyber/; Nathan Freier, "The Emerging Anti-Access/Area-Denial Challenge," (Center for Strategic and International Studies, May 17, 2012).

[12] This definition specifically focuses on denying *states* the ability to access cyberspace. Non-state actors are exceedingly important actors in the international system and particularly in cyberspace, but anti-access warfare strategies have long been the purview of states, city-states, empires, and other recognized political entities that control territory and raise armed forces. The effort to keep individuals and groups out of cyberspace would more likely fall into the realm of law enforcement and domestic control, as opposed to military operations and international relations.

of and dependence on cyberspace is a leading factor in the A2/AD vulnerability.[13] Furthermore, one of the main precepts identified for achieving operational access in the face of armed opposition is to "protect space and cyber assets while attacking the enemy's cyber and space capabilities."[14] As DoD struggles to address A2/AD, policy makers must come to a greater understanding of how cyberspace works, in order to protect US access and potentially deny it to adversaries.

A preliminary examination of the structure of cyberspace suggests the ways that A2/AD can be achieved in that domain. Cyberspace is a global grid that can be manipulated, expanded, and contracted to increase or decrease accessibility. It is comprised of multiple layers, which means that there are different types of vulnerabilities inherent in cyber A2/AD, depending on the layer of cyberspace. Most scholars agree that there are four layers to cyberspace: the physical foundations, the logical layer, the information layer, and the users.[15] The rest of this paper will focus on A2/AD at the physical layer of cyberspace.

3. THE PHYSICAL LAYER OF CYBERSPACE

The physical layer of cyberspace is comprised of physical elements, from fiber optic cables to cell towers, to computers and servers. Of chief importance are the fiber optic cables that traverse the globe, overland and undersea, that transmit data packages from one location to another. In addition to these cables, there are physical nodes of cables (where cables come together) called internet exchange points, and server farms that centralize the processing of data packages and route them to their final destination. In addition to fiber optic cables, there are satellites that are essential to government and commercial communications, although they transmit only a small fraction of the information that flows through cyberspace. Lastly, the electromagnetic spectrum is a constituent part of cyberspace—essential to its functioning and basic operations.

3.1 Cables

3.1.1 Submarine Cables

Submarine cables traverse ocean, sea, and lake floors carrying about 95 percent of all intercontinental telecommunications traffic, in the form of voice and data. International banking and finance activities are highly dependent on these cables, and government and military traffic uses them also. Data and voice communications can be passed via satellite, but it is significantly less expensive and faster to use fiber optic cables. These cables are the fibers that hug the globe and underpin the modern telecommunications system.[16]

There are approximately 1.197 million kilometers of undersea cables.[17] The longest cable systems connect continents, while shorter systems are laid along coastlines to avoid the

[13] U.S. Department of Defense, "Joint Operational Access Concept," (2012), ii.

[14] Ibid., iii.

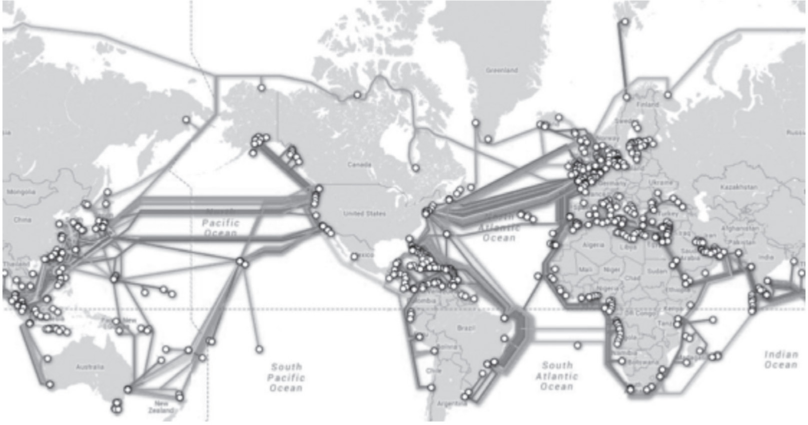
[15] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," in *ECIR Workshop on Who Controls Cyberspace?* (Explorations in Cyber International Relations, Harvard University and Massachusetts Institute for Technology, 2012).

[16] Burnett D. Carter L., Drew S., Marle G., Hagadorn L., Bartlett-MacNeil D., Irvine N., "Submarine Cables and the Oceans - Connecting the World," in *UNEP-WCMC Biodiversity Series* (ICPC/UNEP/UNEP-WCMC, 2009), 3.

[17] Adam Blenford and Christine Jeavans, "After Snowden: How Vulnerable Is the Internet?," *BBC News* January 27, 2014.

problems of terrestrial cables and provide additional resiliency. The highest concentration of cables connects the east coast of the United States with Europe. The largest capacity cables connect New York and the United Kingdom.[18]

FIGURE 1: SUBMARINE CABLE MAP FROM TELEGEOGRAPHY (HTTPS://WWW.ISCPC.ORG/CABLE-DATA/)



Most submarine telecommunications cables are fiber-optic cables, especially newer cable systems. The older coaxial cables are still in use in some places, but their bandwidth capacity is much more limited. Fiber-optic cables have become the primary cable due to increased demand, changes in technology, and reduced cost.[19]

While fiber-optic cables may be relatively new, submarine telecommunications cables are not. The first underwater cable, a copper-based telegraph cable, was laid in 1850 across the Channel to connect the United Kingdom and France.[20] Likewise, tampering with underwater cables is also nothing new. As far back as the Spanish-American War, undersea telegraph cables were destroyed as part of the campaign to sever trans-Atlantic communications links.[21] During the Cold War, the United States famously tapped into Soviet cables to listen to conversations behind the Iron Curtain.[22] More recently, three men were arrested for trying to cut through an undersea cable off the coast of Alexandria, Egypt in 2013.[23] Whether subjected to tampering or destruction, these cables can suffer from unintentional damage as well as sabotage, which threatens to undermine the efficiency, reliability, and security of the global network.

There are approximately 100-150 cable faults or damages every year. Most of the damage that submarine cables suffer is accidental, such as a ship dropping anchor in the wrong place and

[18] U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," (Draft - Version 1, January 15, 2004), 2-3.

[19] Ibid., 1.

[20] Carter L., "Submarine Cables and the Oceans - Connecting the World," 3.

[21] Charles Cheney Hyde, *International Law, Chiefly as Interpreted and Applied by the United States*, 2nd rev. ed., 3 vols. (Boston, MA: Little, Brown and company, 1945), 1956.

[22] Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, *Blind Man's Bluff : The Untold Story of American Submarine Espionage* (New York: Public Affairs, 1998).

[23] "Egypt Arrests as Undersea Internet Cable Cut Off Alexandria," *BBC News*, March 27, 2013 2013.

damaging the cables as they run through shallower waters. Fishing gear such as trawlers are the most common culprit for damage to cables, accounting for roughly half of cable cuts. Over the past five decades, fishing gear and anchors combined represent approximately 70 percent of damage done to submarine cables.[24] As a result, the location of submarine telecommunications cables and their landing stations are often marked on nautical charts and coastal maps, so that ship operators and others may avoid them. These cable cuts happen frequently but most of them are minor and result in little disruption in service.

Submarine cables may also be damaged due to natural disasters and earthquakes. These events represent approximately 12 percent of damage to cables.[25] These events are relatively rare, but they can render catastrophic damage to telecommunications systems. On May 23, 2003, Algeria experienced an earthquake that damaged its telecommunication cables and its satellite ground stations, thus severing almost all of its international telecommunications services. Furthermore, the recurring aftershocks from the earthquake impeded repairs of the submarine cables, which were not completed until June 21, 2003.[26]

Finally, deliberate state action and other human action accounts for approximately 8 percent of cable damage.[27] Human actions may include dredging (such as that associated with beach replenishment), pipeline construction, oil and gas extraction, dumping, and scientific research. Fortunately, cuts near the shore can be repaired relatively quickly because the cables are more accessible. Damage to cables farther out at sea, and at depths of more than 4,000 meters, takes longer to repair and requires specialized equipment.[28]

There is no force tasked with protecting submarine cables, and the responsibility to avoid the cables falls to individual mariners, who are expected to consult the latest charts and abide by local laws to protect cables. In some places, coast guards and navies focused on littoral operations may have an increased responsibility to protect this critical infrastructure because these cables are most vulnerable as they come ashore on the beach head, where they ultimately meet pipes that protect them as they run inland. Thus, maritime military and law enforcement forces (i.e., navies and coast guards) potentially have a role to play in monitoring and protecting critical infrastructure for cyberspace.

3.1.2 Terrestrial Cables

Cable networks that run over land consist of physical lines, transmission line amplifiers, network protection equipment, wavelength termination equipment, and supervisory circuitry.[29] Submarine cables come ashore at cable landing stations, where they are then connected to communications networks on land. Some of these stations are located in densely populated areas, such as New York City, while others are in more remote locations, such as Nedonna Beach, Oregon. At the landing stations, the cables (or fibers, as they are sometimes called) are encased in protective tubes or casings and trenched (i.e., placed in a trench dug for this purpose)

[24] Carter L., “Submarine Cables and the Oceans - Connecting the World,” 45.

[25] Ibid.

[26] U.S. Department of Homeland Security, “Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations,” 7-8.

[27] Carter L., “Submarine Cables and the Oceans - Connecting the World,” 45.

[28] Ibid., 44-47.

[29] U.S. Department of Homeland Security, “Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations,” 6.

or routed along existing rights of way, such as railroad tracks and bridges. Cables, protected by these tubes, bring connectivity inland.[30]

Terrestrial cables are most exposed at the cable landing sites, where they are vulnerable and can be subject to accidental or intentional damage. Common threats to cables include attacks that target the fiber itself, the switching/network control equipment to which it attaches, and the electrical power system that supports it. The cables that are exposed above ground (for instance, from the shoreline to a building or along a right of way) and those that are subterraneous but easily accessible (i.e., below a manhole cover), are most vulnerable to damage.[31]

Cable landing sites often consist of one building with telecommunications equipment. Localized damage to cables and equipment at landing stations is relatively easy to repair, unless the area is unreachable (due to debris, flooding, contamination, or other conditions which may be created by an attack or a natural disaster). The primary security of the cables lies in the resiliency and flexibility of the network. First, the network has "self-healing" powers to reroute traffic away from nodes or pathways. Thus, damage to one cable or landing station is unlikely to have a noticeable effect on routine operations. Second, the cables, landing stations, and other stations are not permanently tied to specific locations and they can be relocated to another place that is more secure.[32] Cyberspace is a partially man-made network, thus we have the ability to change elements of its geographical configuration.

Damage to the landing stations themselves can be conducted directly through a physical attack on the building (such as a bombing or armed assault), indirectly (such as an attack on the power supply), and through internal sabotage (such as a computer virus or worm, fire, or physical damage). Indirect attacks on power sources are unlikely to be successful because landing stations have battery back-up power generator systems, but they are still possible. More likely, a disruption of power to a cable landing station would be part of a larger interruption of service (attack or otherwise) on the regional area.[33]

There are typically minimal forms of physical protection for cable landing sites, making a physical attack possible. Many cable landing sites are completely unprotected, simply small buildings on a beach somewhere. Of those that have some protection, they typically have chain-link fences and basic video surveillance equipment. Thus, as a small area with limited physical barriers it is relatively easy to conduct physical damage to this infrastructure.

Another challenge to managing the vulnerabilities of the physical infrastructure is that the information about the location of cables landing ashore is publically knowable in many places. In the United States, the Federal Communications Commission (FCC) mandates the public availability of licenses for all cables that touch its shores.[34] Furthermore, there are numerous articles discussing risk to critical infrastructure, including cyber infrastructure, which provide

[30] Ibid., 4-6; Andrew Blum, *Tubes: A Journey to the Center of the Internet*, 1st ed. (New York: Ecco, 2012).

[31] U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," 7.

[32] Ibid., 6-7.

[33] Ibid., 7.

[34] Sam Biddle, "How to Destroy the Internet," Gizmodo.com, http://gizmodo.com/5912383/how-to-destroy-the-internet.

specific information about the location of some of the infrastructure.[35] In addition, it is not difficult to obtain the equipment to find a cable line underground and destroy it–a line tracer and an axe will suffice. Despite this, the interconnectedness of land networks provides resiliency for the system.[36]

3.2 Satellites

Satellites are another essential part of cyberspace, but they transmit only 5 percent of voice and data telecommunications. When compared with fiber optic cable networks, they are five times slower and have 0.3 percent of the capacity. They are also more than 50 times more expensive per megabits per second. Furthermore, the design lifespan of satellites is 10-15 years, whereas it is 25 years for cables.[37]

TABLE 1: COMPARISON OF SATELLITES AND SUBMARINE FIBER OPTIC CABLES ACROSS SEVERAL KEY FACTORS IN TELECOMMUNICATIONS.[38]

Comparison Factor	Satellite	Optical Subsea
Latency	250 milliseconds	50 milliseconds
Design Life	10-15 years	25 years
Capacity	48,000 channels	160,000,000 channels
Unit cost per Mbps capacity	$737,316 US	$14,327 US
Share of traffic: 1995	50%	50%
Share of traffic: 2008	3%	97%

Private sector communications satellites provide an array of service, including voice and internet service. These satellites usually orbit in Middle Earth Orbit, a distance of 200 to 930 miles from Earth. The larger the satellite, the greater the power capacity, and thus the higher an orbit it is capable of achieving. The major players in private sector communications satellites are ViaSat, Space Systems/Loral, O3b, Eutelsat, and IntelSat.[39]

Satellite access faces several challenges for end users, in particular: high cost, signal latency, signal strength, and interference. With regards to the economics of satellites, they have high upfront costs ($50 to $400 million dollars for a large satellite)[40] and marginal returns, particularly communications and internet satellites that are competing with the more efficient cables that have much faster rates of transmission.[41] Signal strength and integrity are also an issue; due to interference and power requirements for satellites, signal reliability can be unstable.

[35] Paul Saffo, "Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability," International Relations and Security Network (ISN), http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=162869.

[36] Blenford and Jeavans, "After Snowden: How Vulnerable Is the Internet?."

[37] John K. Crain, "Assessing Resilience in the Global Undersea Cable Infrastructure" (Naval Postgraduate School, 2012), 3.

[38] Ibid. Adapted from C. Donovan, "Twenty thousand leagues under the sea: A life cycle assessment of fibre optic submarine cable systems" Masters Thesis, The Royal Institute of Technology, Stockholm, Sweden, 2009.

[39] Alistair Barr and Andy Pasztor, "Google Invests in Satellites to Spread Internet Access," *The Wall Street Journal* June 1, 2014.

[40] "The Cost of Building and Launching a Satellite," http://www.globalcomsatphone.com/hughesnet/satellite/costs.html.

[41] Latency is the measure of response time, but the "speed" of a network commonly refers to throughput/bandwidth.

Additionally hardware capability is particularly important for satellites. Satellite manufacturing is a time-consuming process and it requires significant lead time, such as five to ten years for larger satellites. Following Moore's Law, rapid improvement in technological capabilities means that by the time satellites are launched, their hardware may already be out-of-date. Microsatellites, which can be developed in one to two years at a cost of only a few million dollars, may be a solution to this problem.[42]

Satellites face vulnerabilities in space and on the ground. In space, their primary challenges include missiles, space debris, and hacking. On the ground, their control stations are physical targets that can be compromised by deliberate action, accidental causes, or acts of nature.

Anti-satellite missile systems have been a threat since the 1950s and they continue to be developed today. In 2007, China demonstrated its anti-satellite missile capability by destroying a defunct weather satellite at 537 miles above Earth. Similarly, the United States destroyed a spy satellite in 2008 at 150 miles above Earth.

Space debris is also a threat to satellites. Debris is created by man-made objects in space, including old satellites, spent rocket stages, and fragments from erosion, collision, and disintegration of items in orbit. In 2009, the U.S. Iridium 33 communications satellite collided with a defunct Russian military communications satellite Cosmos 2251. The collision caused a significant increase in debris, requiring the International Space Station to execute avoidance maneuvers.[43] Likewise, the aforementioned Chinese weather satellite that was destroyed in 2007 resulted in significant debris due to the way in which it was shot down.[44]

Satellite hacking has already been reported.[45] Given that satellites are often sent up with outdated technology, vulnerabilities are likely to grow over time. The technological expertise required to hack a satellite may be found within state resources and armed forces, as well as within the hacking community. Indeed, China was accused of hacking into U.S. weather satellites in 2014[46], but there are also claims of blackhat and whitehat hackers hacking satellites.[47]

Satellite communications relies on ground stations to receive information and track satellites moving through orbit. The ground stations function as a hub to receive information from the satellite and connect it with terrestrial communication networks, such as the internet. Ground stations can also be used to upload computer programs or issue commands to the satellite. These stations are susceptible to physical attack as well as natural events, such as earthquakes, tornadoes, and tsunamis.

[42] Conrad de Aenlle, "U.K. Firm Finds Niche in 'Discount' Satellites" *The New York Times* June 19, 2001

[43] "International Space Station Again Dodges Debris," *Orbital Debris Quarterly News, National Aeronautics and Space Administration* 15, no. 3 (July 2011).

[44] "Chinese Asat Test," Center for Space Standards & Innovation, http://www.centerforspace.com/asat/.

[45] Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," *Washington Post* November 12, 2014.

[46] Ibid.

[47] Stephen Northcutt, "Are Satellites Vulnerable to Hackers?," http://www.sans.edu/research/security-laboratory/article/satellite-dos.

4. IMPLICATIONS FOR CYBER SECURITY

It is clear from the previous assessment that the physical infrastructure of cyberspace can be degraded or destroyed in a way that would prevent an adversary from accessing the contested area (in the case, cyberspace) and/or, if the enemy is already present, to diminish its capacity to maximize its capabilities.

In order to completely deny an enemy access to cyberspace, the opposing force would first need to drive the enemy out of cyberspace. In this way, cyber A2/AD is significantly different from A2/AD in other domains because of its compression of time and space. Countries already have a presence in the domain and have immediate access to all parts of cyberspace. This is in stark contrast to the maritime domain, for example, where a ship launched in the Atlantic Ocean does not have immediate access to Straits of Malacca. Thus, A2/AD in the maritime domain would involve preventing entry to a specific region within the domain; in cyberspace, it is necessary to cut off their access to the domain entirely.

States can be cut off from cyberspace through attacks on the physical infrastructure that connects them to the grid. The cables that connect them to other countries, whether terrestrial or submarine, must be damaged or destroyed and satellites and/or their ground stations must be compromised and rendered non-functional. At this point, the country would be isolated from the international community and A2/AD could be maintained by preventing the country from re-establishing connectivity. For those who wanted to go further and prevent a country for communicating internally, domestic internet exchange points and server farms would be the next targets.

The decision to stop at isolation or continue to domestic communications depends on the goal of the attack and the broader context. If it is part of a military campaign that is expected to be quick, then isolation would likely be sufficient to degrade military capabilities and diminish command and control. If the goal requires a more extensive campaign that will likely meet with significant resistance, then attacking domestic infrastructure will weaken the state by attacking the centres of gravity, and accelerate the collapse of the state.

4.1 Strategy Implications

Cyberspace communications nodes are centres of gravity in the modern era. The ability to hold cyberspace infrastructure and communication nodes at risk is a significant factor in a conflict environment. Governments rely on cyberspace communications for command and control of military forces, economic stability, and societal well-being. Without access to cyberspace, the economy would immediately come to a halt, with millions of dollars lost each day of non-connectivity. Government, law enforcement, and security forces would have a difficult time functioning and protecting the population from domestic or foreign threats. Societal functioning would grind to a halt as people would need to develop alternate methods of doing just about everything.

Because of the serious impact of a cyber A2/AD strategy for society as a whole, it is likely that it would be applied during a military conflict, as one element of a larger campaign. At any threshold lower than armed conflict, cyber A2/AD presents the risk of potentially escalating the existing crisis to the level of armed conflict, as states could perceive the A2/AD strategy as a threat to their defences, economies, and societies.

Traditional deterrence strategies are useful to consider for preventing A2/AD in cyberspace. Deterrence is intended to convince an adversary not to take an action by leading the adversary to believe that the costs required to take the action would exceed the potential benefits derived from the action. Deterrence can be accomplished by three different means: punishment, denial, and cooperation.[48]

Deterrence by punishment occurs when the actor signals that the costs inflicted in retaliation for being attacked would outweigh the potential gains derived from launching an attack. Successful deterrence therefore depends on the actor being able to credibly threaten offensive actions in order to ensure the desired response.

In cyberspace, attribution poses a significant problem for deterrence by punishment. It is essential that states have the capability to correctly attributing the attack in order to deter potential adversaries. Without the ability to attribute the attack, there would be no way to punish the attackers. Attribution is difficult in cyberspace, but it becomes more achievable in certain contexts and when traditional intelligence methods are also utilized.[49] However, if A2/AD in cyberspace takes place during a military conflict, then attribution is no longer a problem.

A second challenge for deterrence by punishment for cyber A2/AD is that punishment itself may be difficult to achieve precisely because cyber technologies underpin the many of the capabilities that military forces may use to retaliate. A likely reason for a state to attempt cyber A2/AD against the state like the United States would be to degrade its overall military capacity, as well as prevent it from launching cyber operations. As a result, military retaliation for an A2/AD attack in cyberspace may not a viable option, and punishment may have to come from a source that was not cyber-dependent, such as political or economic sanctions.

If a state retains the capability to retaliate through kinetic or non-kinetic means, there is the issue of credibility—whether or not state seeking to deter has the capabilities to harm the adversary through kinetic or non-kinetic means. In addition, there may be a question of whether a state would follow through with a kinetic attack in response to a non-kinetic, cyber attack.[50]

Deterrence by denial is defensive and deterrence is preventive, but they both have the same ultimate goal of seeking to deny benefits of attack. Deterrence by denial is achieved through a display of capabilities that suggest the probability of succeeding in the attack is quite low. It can be achieved by reducing the vulnerabilities through hardening, redundancy, training, and continuous vulnerability analysis.[51]

[48] Christopher Wrenn, "Strategic Cyber Deterrence" (Tufts University, 2012), 166-68.

[49] Richard J. Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependecies," (Center for a New American Security).

[50] Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," (Cyber Security Policy and Research Institute: The George Washington University, 2011).

[51] Wrenn, "Strategic Cyber Deterrence," 171.

Deterrence by denial has some advantages in cyberspace. The infrastructure of cyberspace since its earliest days has been designed for resiliency. While much of the physical infrastructure of cyberspace is relatively unprotected, located on beaches, along railways, and in buildings in densely populated areas, very little of that critical infrastructure is critical by itself. The nodes and cables may be relatively exposed and potentially vulnerable, none is singularly important to the entire system.

The infrastructure consists of redundant cables and satellites for private sector communications and military operations. The logic programming of the data and telecommunications was designed to adapt to changing circumstance, to automatically route traffic through an alternate route when the first route is unavailable. This "self-healing" property of cyberspace makes it difficult to cause substantial damage without launching a full assault against the infrastructure.

A full assault on the physical infrastructure of cyberspace would require substantial effort to target satellites and their ground stations, cables, servers, internet exchange points, and any activities within the electromagnetic spectrum. The difficulty of conducting this type of assault varies depending upon the target country. For a country that connects to cyberspace in relatively few places, such as North Korea, this may be achievable. However, for countries with a greater number of connections, such as the United States or the United Kingdom, it would be much more difficult to target all of their cables and satellites.

The downsides of deterrence by denial is that it is expensive to harden vulnerabilities and create (and maintain) redundancies. Many states or private industries may be unable, unwilling, or reluctant to invest resources in redundant capabilities instead of other more profitable ventures.

Deterrence by cooperation seeks to prevent an attack through interdependencies, norm creation, international law, and international agreements. Interdependency create networks that can be leveraged to influence the costs and benefits of a cyber attack. Norms can create a common standard for conduct that can help keep up with the rapid pace of technological development. International laws can deter, while international agreements can help to regulate cyber matters between and among states.[52]

Successful deterrence in cyberspace requires all three elements: punishment, denial, and cooperation. These elements work together to increase the costs (and difficulty) of a cyber attack beyond the desired benefit of the attack. Conversely, if there is little to no real cost to the adversary if the attack fails, then it has very little to lose by attempting attacks.[53] Fortunately, states do not need to deter all potential cyber attackers, only those that can cause the most harm. There may not be one formula of deterrence for all actors, but rather deterrence may need to be tailored to the threat or adversary. For some actors, punishment may need to play a more prominent role, whereas denial or cooperation may need to be more prominent to deter other actors.[54]

[52] Ibid., 172.

[53] Glaser, "Deterrence of Cyber Attacks and U.S. National Security."

[54] Wrenn, "Strategic Cyber Deterrence," 166-72.

5. CONCLUSIONS AND RECOMMENDATIONS FOR POLICY MAKERS

This paper has demonstrated that strategic A2/AD at the physical layer of cyberspace is possible and would pose significant problems for military and economic power of the targeted state. Deterrence would require the threat of credible punishment, denial, and cooperation to be most effective. Each element of the triad has costs and weaknesses associated with it, but collectively they provide for the most robust deterrence.[55]

Given that several states have already issued policies articulating their potential responses to cyber attacks, or they have already engaged in actions that make their policies clear, deterrence by punishment is already underway. Further actions by policy makers may include articulating clearly defined "red lines", establishing thresholds to issue and carry out threats, and consideration for retaliation and resistance to attacks.

The next recommendation for policy makers is to invest in resiliency and redundancy to counter a potential A2/AD strategy. This recommendation is particularly important in an era of fiscal constraints and persistent budget cuts within defence departments in many countries. Despite budgetary concerns, investment in redundant and resilient physical infrastructure is a key element to ensuring that all other military capabilities are able to operate as planned. Assured access to cyberspace underpins nearly all activities of advanced militaries. Investment in infrastructure will also have several non-military benefits. There is an immediate economic benefit to the private sector companies that make satellites, cables, and server farms. In addition, it can spur innovation and upgrades for government and civilian networks alike.

The final recommendation for policy makers and scholars alike is to define the norms for codes of conduct for states and their citizens to follow. States may agree to cooperate with each other at the international level, but norms embedded in values and social structures are essential to bring the society in line with to the official policies, so that states can effectively deter their own populations from engaging in counter-norm behaviour.[56] In particular, norm generation paired with redundancy can provide for much great resistance and lessen vulnerability to A2/AD in cyberspace.

REFERENCES

Aenlle, Conrad de. "U.K. Firm Finds Niche in 'Discount' Satellites " *The New York Times*, June 19, 2001

Albanesius, Chloe. "Internet in North Korea Offline after Apparent Attack." PC Magazine, http://www.pcmag.com/article2/0,2817,2474065,00.asp.

Barr, Alistair, and Andy Pasztor. "Google Invests in Satellites to Spread Internet Access." *The Wall Street Journal*, June 1, 2014.

Biddle, Sam. "How to Destroy the Internet." Gizmodo.com, http://gizmodo.com/5912383/how-to-destroy-the-internet.

[55] Ibid., 170.
[56] Ibid., 169.

Blenford, Adam, and Christine Jeavans. “After Snowden: How Vulnerable Is the Internet?” *BBC News*, January 27, 2014.

Blum, Andrew. *Tubes: A Journey to the Center of the Internet*. 1st ed. New York: Ecco, 2012.

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-MacNeil D., Irvine N. “Submarine Cables and the Oceans - Connecting the World.” In *UNEP-WCMC Biodiversity Series* ICPC/UNEP/UNEP-WCMC, 2009.

Castells, Manuel. *Communication Power*. New York: Oxford University Press, 2009.

“Chinese Asat Test.” Center for Space Standards & Innovation, http://www.centerforspace.com/asat/.

Choucri, Nazli, and David D. Clark. “Integrating Cyberspace and International Relations: The Co-Evolution Dilemma.” In *ECIR Workshop on Who Controls Cyberspace?*: Explorations in Cyber International Relations, Harvard University and Massachusetts Institute for Technology, 2012.

“The Cost of Building and Launching a Satellite.” http://www.globalcomsatphone.com/hughesnet/satellite/costs.html.

Crain, John K. “Assessing Resilience in the Global Undersea Cable Infrastructure.” Naval Postgraduate School, 2012.

Danzig, Richard J. “Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America’s Cyber Dependecies.” Center for a New American Security.

“Egypt Arrests as Undersea Internet Cable Cut Off Alexandria.” *BBC News*, March 27, 2013 2013.

Flaherty, Mary Pat, Jason Samenow, and Lisa Rein. “Chinese Hack U.S. Weather Systems, Satellite Network.” *Washington Post*, November 12, 2014.

Freier, Nathan. “The Emerging Anti-Access/Area-Denial Challenge.” Center for Strategic and International Studies, May 17, 2012.

Glaser, Charles L. “Deterrence of Cyber Attacks and U.S. National Security.” 8. Cyber Security Policy and Research Institute: The George Washington University, 2011.

Hyde, Charles Cheney. *International Law, Chiefly as Interpreted and Applied by the United States*. 2nd rev. ed. 3 vols Boston, MA: Little, Brown and company, 1945.

“International Space Station Again Dodges Debris.” *Orbital Debris Quarterly News, National Aeronautics and Space Administration* 15, no. 3 (July 2011 July 2011): 1.

Kazianis, Harry. “The Real Anti-Access Story: Cyber “ *Flashpoints: Diplomacy by Other Means* (2013). Published electronically May 15, . http://thediplomat.com/flashpoints-blog/2013/05/15/the-real-anti-access-story-cyber/.

Northcutt, Stephen. “Are Satellites Vulnerable to Hackers?” http://www.sans.edu/research/security-laboratory/article/satellite-dos.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Russell, Alison Lawlor. Cyber Blockades. Washington DC: Georgetown University Press, 2014.

Saffo, Paul. “Disrupting Undersea Cables: Cyberspace’s Hidden Vulnerability.” International Relations and Security Network (ISN), http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=162869.

Sontag, Sherry, Christopher Drew, and Annette Lawrence Drew. *Blind Man’s Bluff: The Untold Story of American Submarine Espionage*. New York: Public Affairs, 1998.

Tangredi, Sam J. *Anti-Access Warfare: Countering A2/Ad Strategies*. Annapolis, Maryland: Naval Institute Press, 2013.

U.S. Department of Defense. "Joint Operational Access Concept." 2012.

U.S. Department of Homeland Security. "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations." Draft - Version 1, January 15, 2004.

Wrenn, Christopher. "Strategic Cyber Deterrence." Tufts University, 2012.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Blackout and Now? Network Centric Warfare in an Anti-Access Area-Denial Theatre

Robert Koch
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
robert.koch@unibw.de

Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
mario.golling@unibw.de

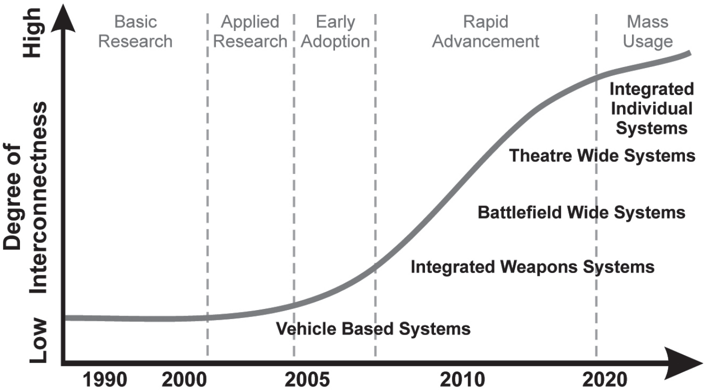
Abstract: The advance of information and communication technology nowadays offers world-wide broadband communication with high data rates. Motivated by the benefits of real-time distributed information shared between units as well as different levels of command for the purpose of fast and reliable decision-making, numerous nations have been working hard over the past years to implement Network Centric Warfare (NCW). By that, information superiority can be gained and translated into command superiority and finally into force superiority. Being strongly dependent on fast and reliable communication, electrical power outages or disruptions of network nodes like SatCom systems respectively links can have a severe impact on information gathering and in turn on the decision making process and the capacity of forces to act. As a consequence, questions arise about the robustness of the NCW doctrine. The ability of power projection is strongly hampered by anti-access/area denial (A2/AD) capabilities. In order to successfully conduct military operations against technologically advanced opponents, forces must address A2/AD as an important element of today's battle-field, comprehend the associated operational implications, and eliminate any imbalances between military objectives and the means by which to achieve them. Following these considerations, this paper - on a technical level - analyses capabilities and weaknesses of NCW with regard to modern theatres. Based on that, recommendations in order to strengthen the performance and reliability for the further development of NCW are given.

Keywords: *Network Centric Warfare, cyber war, A2AD, anti-acess area denial, network breakdown, next-generation military networks, robust NCW.*

1. INTRODUCTION

In recent years, Information and Communication Technology (ICT) has significantly changed our daily life. Today, in one way or another, almost every one of us is affected by ICT. Terms such as Smart Grid, Smart City or Industry 4.0 are only a few examples of how we are dependent on the availability of ICT. Of course, these developments also affect the military. Starting in the early 1990s, the military has been thinking of how the use of ICT can increase the efficiency of forces. One of the first ones who asked themselves how the battlefield of the 21st century will look alike was the US Navy (e.g., see [1]). The main consequence of these considerations is the increased integration of individual, previously autonomously acting systems (see Figure 1). This technical integration has finally led to the concept of Network Centric Warfare (NCW). NCW is a *theory, which proposes that the application of information age concepts to speed communications and increase situational awareness through networking improves both the efficiency and effectiveness of military operations* [2]. As such, NCW creates information superiority by means of a network of reconnaissance, command and control as well as weapon systems and thus ensures the military superiority across the entire range of military operations (full spectrum dominance). The vision for Network Centric Warfare is to provide seamless access to timely information at every echelon in the military hierarchy. This enables all elements, including individual infantry soldiers, ground vehicles, command centres, aircraft and naval vessels, to share information to be combined into a coherent, accurate picture of the battlefield.

FIGURE 1: INTEGRATION OF PREVIOUSLY AUTONOMOUS SYSTEMS IN THE MILITARY (BASED UPON [3])



Proponents argue that the concept of "*strong and flexible network linked military forces*" allows combat units (i) to be smaller in size, (ii) to operate more independently and effectively, (iii) to undertake a different range of missions, (iv) to prevent or reduce fratricides and (v) to speed up the pace of warfare in comparison to non-networked forces [2]. NCW will also produce

(i) improved understanding of higher command's intent, (ii) improved understanding of the operational situation at all levels of command and (iii) increased ability to tap into the collective knowledge of all forces to reduce the "fog and friction" [2]. With the increasing significance, implementation and application of NCW, in particular the following endangerments are rising: Being heavily dependent on the availability and capability of communication between all nodes, the underlying networks represent one of the weakest links of the chain.

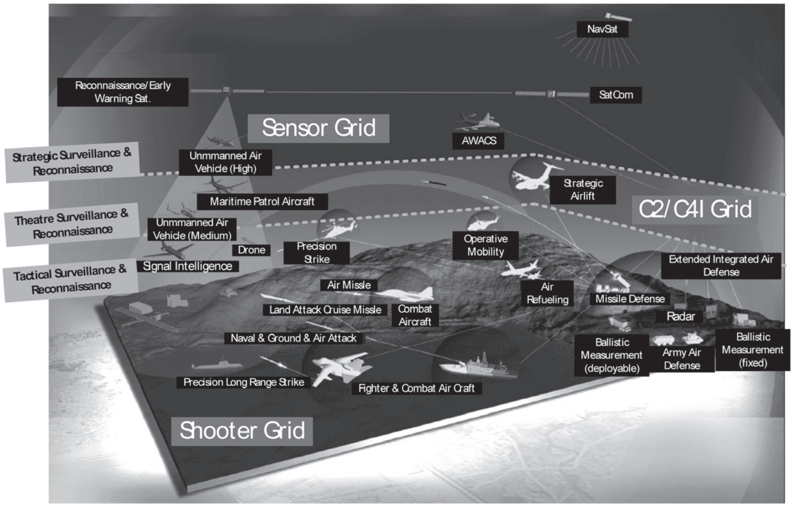
Following these considerations, this paper – on a technical level – analyses capabilities and weaknesses of NCW with regard to modern theatres. On this basis, recommendations in order to strengthen the further development of NCW are given. Therefore, the rest of the paper is structured as follows: First, a deeper introduction into the concept of NCW is given in Section 2. Following this, Section 3 concentrates on the technical capabilities. Here, a brief description of current as well as upcoming technologies and technical trends relevant for communication is given. Section 4 of the paper gives a comprehensive overview of advantages, risks and shortcomings of NCW. Section 5 addresses upcoming advances in ICT. Next to this, Section 6 outlines requirements for the further development of NCW derived from the preceded analysis, supporting the usability of NCW in a contested environment. Based upon that, possibilities for future developments of NCW are described. Finally, Section 7 concludes the paper.

2. THE CONCEPT OF NETWORK CENTRIC WARFARE

The basic element of NCW is gaining information superiority and thereby, command and force superiority by the use of networked sensor grids, high-quality information backplanes, engagement grids and (partly automated) Command and Control (C2) / Command, Control, Communications, Computers, and Intelligence (C4I) processes (see Figure 2) [4].

Vast financial resources have been invested by numerous countries to modernize their ICT and to enable NCW capabilities. Despite these high efforts, this process is currently not completely finished, yet, not even in the US armed forces. While the huge ICT investments of the U.S. DoD already enable information superiority [5], the target structures for full operational capability are not realized completely, yet. For example, the modernization program for tactical networks of the U.S. Army including full networking on-the-move and airborne communication nodes is re-scheduled from 2019 to 2028 [6]. In order to realize a sustainable network structure, open standards and system descriptions are available (e.g., see [7]), motivating industry to develop and provide required systems and components on an affordable base. Furthermore, even with already available ICT capabilities, the NCW theory is often only processed as a transformational concept and has not been adapted extensively to the doctrines, yet. In addition, old-fashioned thinking and resistance to NCW theory hampers an activation of the full power of information superiority [5].

FIGURE 2: WEAPON SYSTEMS, COMMAND AND CONTROL AND A SENSOR GRID ARE INTERCONNECTED WITH ONE ANOTHER TO ALLOW FOR MAXIMUM EFFICIENCY BETWEEN EACH OTHER (ADAPTED ON THE BASIS OF [8])


NavSat
Reconnaissance/Early Warning Sat.
SatCom
Sensor Grid
AWACS
Strategic Surveillance & Reconnaissance
Unmmanned Air Vehicle (High)
Strategic Airlift
Maritime Patrol Aircraft
C2/C4I Grid
Theatre Surveillance & Reconnaissance
Unmmanned Air Vehicle (Medium)
Drone
Precision Strike
Operative Mobility
Extended Integrated Air Defense
Tactical Surveillance & Reconnaissance
Signal Intelligence
Air Missle
Air Refueling
Missile Defense
Land Attack Cruise Missle
Combat Aircraft
Radar
Naval & Ground & Air Attack
Ballistic Measurement (deployable)
Army Air Defense
Ballistic Measurement (fixed)
Precision Long Range Strike
Fighter & Combat Air Craft
Shooter Grid

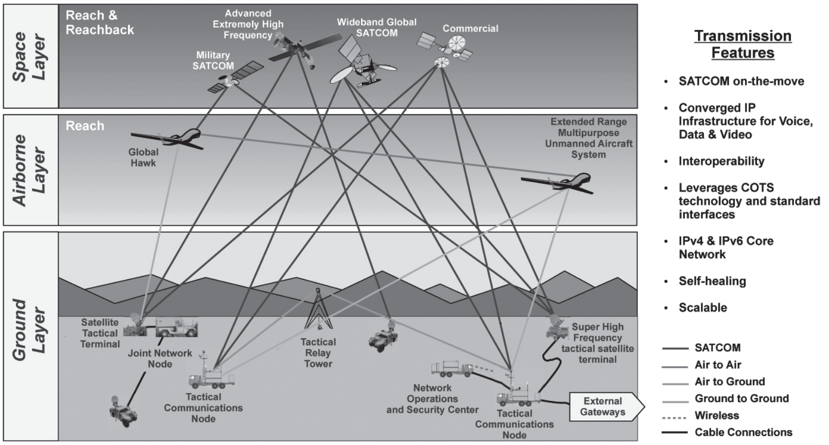
3. TECHNICAL IMPLEMENTATION OF NETWORK CENTRIC WARFARE

C4I-capabilities are the nervous system of the military. As such, NCW relies on a high-bandwidth communications backbone consisting of fibre optics and satellites, all communicating using the Internet Protocol (IP) [2]. Furthermore, NCW is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms [2]. Parts of the NCW technology rely on line-of-sight radio transmission for microwave, infrared signals or laser beams and microwave towers, or both low-altitude and high-altitude satellites. The architectures must also have the ability to dynamically self-heal and re-form the network when one or more communications nodes are interrupted [4]. Satellites are crucial for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, a missile warning capability, and a capability to "reach back" to the home country for support [9, 1]. Here, comparatively high requirements are imposed on the data rate. Within the Operation Iraqi Freedom in 2003 for instance, the individual data rate of 64 kilobits per second was considered as too small for the needs of the army [2].

A. Anti-Access Area-Denial (A2/AD)

Modern forces are highly dependent on space assets. As described in a report to the US congress [2], the United States remains highly dependent on space assets, and has enjoyed space dominance during previous Gulf conflicts largely because its adversaries simply did not exploit space, or act to negate U.S. space systems. In case of a technologically advanced adversary, this dependency created by NCW can therefore result in an Achilles' heel. Forces must be prepared to deploy to a wide range of locations that include almost any type of terrain and confront adversaries that span the threat spectrum from very poorly armed bands to peer-level foes [10]. In this context, the term A2/AD refers to all actions to limit the ability of power projection of an opponent. Anti-access (A2) challenges prevent or degrade the ability to enter an operational area [10]. These challenges can be geographic, military, or diplomatic. Area denial (AD) refers to threats to forces within the operational area [10]. In addition to conventional attacks, in particular AD also includes attacks in cyberspace.

FIGURE 3: SIMPLIFIED MODEL OF A NCW INFORMATION NETWORK (NAVY AND AIR FORCE HAVE BEEN OMITTED FOR SIMPLICITY; IMAGE BASED ON [6])


Space Layer
Reach & Reachback
Advanced Extremely High Frequency
Military SATCOM
Wideband Global SATCOM
Commercial
Airborne Layer
Reach
Global Hawk
Extended Range Multipurpose Unmanned Aircraft System
Ground Layer
Satellite Tactical Terminal
Joint Network Node
Tactical Communications Node
Tactical Relay Tower
Network Operations and Security Center
Tactical Communications Node
Super High Frequency tactical satellite terminal
External Gateways
Transmission Features
• SATCOM on-the-move
• Converged IP Infrastructure for Voice, Data & Video
• Interoperability
• Leverages COTS technology and standard interfaces
• IPv4 & IPv6 Core Network
• Self-healing
• Scalable
SATCOM
Air to Air
Air to Ground
Ground to Ground
Wireless
Cable Connections

B. NCW Scenario

For the further analysis of NCW requirements and endangerments, the scenario depicted in Figure 3 will be used; because of the focus of the paper, only technical capabilities are described: Two capable enemies have both realized full operational capabilities of NCW, therefore comprehensively connected units with regard to networks and satellite communication (SatCom) systems.

Both parties possess Electronic Warfare (EW) capabilities in all major subdivisions, namely Electronic Attack (EA), Electronic Protection (EP) and Electronic Warfare Support (EWS). As written in the Joint Publication 3-13.1, "Electronic Warfare" [11], EA is, e.g., the use of electromagnetic energy to neutralize or destroy enemy combat capabilities. EP are actions taken to protect personnel, facilities and equipment from any effects of the use of EM spectrum, while EWS contains actions to search for, intercept, identify and locate radiated EM energy. Therefore, they are able to influence the enemies' actions while protecting the own ones. Both parties are able to execute Computer Network Operations (CNO), namely executing Computer

Network Attacks (CNA) to, e.g., disrupt, deny or destroy information within computer systems and computer networks on the one hand and to protect and monitor networks to detect and respond to network attacks and intrusions by means of Computer Network Defence (CND) on the other hand. See Table 1 respectively Figure 4 for an overview of the different terms. Within a NCW scenario, this presents both, a major chance to manipulate and disrupt systems of the enemy, therefore destroying his NCW capability and hence his information and force superiority. Otherwise, the own dependency on a working NCW system forces a strong protection and capable redundancy to repel attacks of the enemy and keep the superiority.

Beside satellite capabilities, further communication assets can be placed in the airborne layer by the use of, e.g., Unmanned Aerial Vehicles (UAVs). The relevance of secure and capable links can be illustrated with a look at UAVs. E.g., the connection and operation of UAVs requires extensive link capabilities of up to 50 Mbps per unit, where a disruption of the link can have severe effects on the success of the mission. Another example is the use of Special Operation Forces (SOF), which are a strategic asset and therefore heavily dependent on reliable communication links. While link data rates of about 256 to 512 Kbps have been satisfactorily for several years, new sensor technology and an increasing need for extensive data exchange within NCW raise the requirements for data rates dramatically. E.g., while the return link of a Predator UAV started with 3.2 Mbps, a Global Hawk already requires about 50 Mbps today, while possibly reaching 274 Mbps in the near future [15].

FIGURE 4: GRAPHICAL DISTINCTION BETWEEN THE TERMS

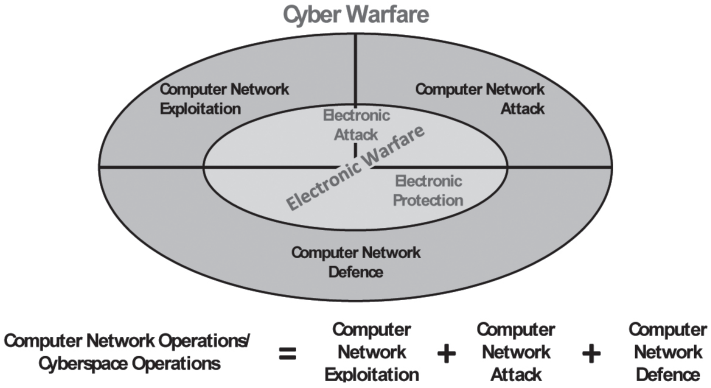


TABLE1: OVERVIEW OF ABBREVIATIONS.

Abbreviations	Definition
Network Centric Warfare (NCW)	Theory that proposes the application of information age concepts to speed communications and increase situational awareness through networking and in turn improves both the efficiency and effectiveness of military operations [2].
Anti-Access (A2)	Corresponds to means which try to prevent or degrade the ability to enter an operational area [10]. These challenges can be geographic, military, or diplomatic.
Area Denial (AD)	Refers to threats to forces within the operational area. AD threats are characterized by the opponent's ability to obstruct the actions of forces once they have deployed [10].
Electronic Warfare (EW)	Refers to any action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the enemy. EW includes three major subdivisions: Electronic attack (EA), Electronic Protection (EP), and Electronic Warfare Support (EWS) [11].
Electronic Attack (EA)	The use of electromagnetic energy to neutralize or destroy enemy combat capabilities [11].
Electronic Protection (EP)	Actions taken to protect personnel, facilities and equipment from any effects of the use of EM spectrum [11].
Electronic Warfare Support (EWS)	Actions to search for, intercept, identify and locate radiated EM energy [11].
Cyber Warfare (CW)	The unauthorized conducting of a penetration - including the preparation - by, on behalf of, or in support of, a government into another nations' computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, falsify or delete data, or cause the disruption of or damage to a computer or network, or the objects a computer system controls (such as SCADA-systems "supervisory control and data acquisition") [12].
Computer Network Operations (CNO) / Cyberspace Operations (CO)	The employment of cyber capabilities where the primary purpose ist to achieve objectives in or through cyberspace [13].
Computer Network Attacks (CNA)	Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves [14].
Computer Network Defense (CND)	Includes actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks [14].
Computer Network Exploitation (CNE)	Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks [14].

4. THREATS FOR NETWORK CENTRIC WARFARE

As shown before, NCW enables advantages by providing an improved situational awareness of the environment, a better understanding of the operational situation, a dramatically accelerated decision-making as well as a higher mission effectiveness. On the other hand, several risks are inducted by the dependency on capable and reliable communication networks. The decision, if a risk can be taken, depends on a comprehensive risk analysis: if a weakness or vulnerability is indeed existent, but not exploitable by the enemy, it presents no endangerment for the system respectively operation. Unfortunately, such an absolutely statement is typically not possible in the real-world; often, one only can estimate the risk, e.g., based on intel information, and then decide if the risk can be accepted. For example, the NIST Special Publications 800-39, "Managing Information Security Risk" [16] and 800-30, "Guide for Conducting Risk Assessments" [17], are giving guidance how to establish programs for managing information security risk.

Referring to the scenario, two highly capable enemies are confronted, resulting in high risks that the enemy will attack NCW capacities; vice versa, attacking the enemy's NCW structure can open up an advantageous situation for oneself. Therefore, significant threats to NCW are discussed as follows:

Anti-Satellite: Satellites are fully integrated, essential components of NCW as they are the only systems able to provide a continuous, worldwide broadband network supply. Being placed comparatively secure on different orbital positions, these systems are nevertheless threatened nowadays. The first Anti-Satellite Weapon (ASAT) was launched on May 24, 1962 by the U.S; a shortly ensuing exoatmospheric test of a nuclear ASAT was conducted on July 9, 1962 [18]. After that, the Partial Nuclear Test Ban Treaty (LTBT) from 1963 bans nuclear weapons testing including the atmosphere and outer space, the Outer Space Treaty from 1967 denies the placing of "any objects carrying nuclear weapons or any other kinds of weapons of mass destruction" [19] while the Anti-Ballistic Missile Treaty of 1972 denies the development, test and deployment of ABM systems, inter alia air-based and space-based. The contracts do not deny the development and deployment of ASATs completely; for example, a two-staged anti-satellite missile with infrared homing capability that was air-launched in high altitude from a F-15 was developed in the 1970s [18]. Lately, China demonstrated the relatively simple deployment of a Kinetic Kill Vehicle (KKV), which was engaged by a road-transportable, two-staged CSS-5 rocket and which was used to successfully destroy the Chinese weather satellite Fengyun-1C (FY-1C) on January 11, 2007 [20].

Another endangerment of satellites is the increasing amount of debris: scattered parts of destroyed or broken satellites and systems, rocket firing steps, etc. For example, the destruction of FY-1C produced numerous fragments, now circulating in different orbits. The Space Surveillance Network (SSN, [21]) has registered 3037 objects resulting from the FY-1C collision and scientists of the NASA Orbital Debris Program Office presume 35000 additional objects about 1 cm or more, which are not tracked at the moment [22]. Calculations predict, that only approx. 6% of the fragments of FY-1C will enter Earth's atmosphere until 2017, while 79% will remain in orbit until 2109. Debris presents high risks for the operation of satellites; e.g., the Russian micro-satellite BLITS (Ball Lens in The Space) was hit by a fragment of FY-1C on January 22, 2013 and likely destroyed [23]. Another example is the destruction of the operative communication satellite Iridium 33, which had been hit and destroyed by the non-active Russian communication satellite Cosmos 2251 on February 10th, 2009 [24]. Beforehand, the closest approach of Iridium 33 and Cosmos 2251 was calculated to be approx. 584 m [25], which shows the possibility of error of these methods. The development of new, powerful laser system of reduced sizes (e.g., see [26]) enable the construction and deployment of new ASAT system, but also the design of new protection and active defence capabilities for satellites.

Malicious hard- and software: Because of the steady cutback of defence budgets in most countries after the end of Cold War (the so-called peace dividend), but also in the context of the financial crisis, armament projects are often reduced and financially limited. As a consequence, in-house developments are not possible any longer (besides a few exceptions, e.g., crypto devices) and Commercial, Governmental and Military off-the Shelf (COTS/GOTS/MOTS) products are used comprehensively to reduce R&D and system costs, especially in the area of ICT products. While this reduces costs and enables better performance on the one hand, these products are hardly controllable, fraught with risk to infiltrate highly sophisticated and hardly detectable Trojan circuits and hardware backdoors into high security environments. Especially state-of-the-art weapon systems typically contain numerous COTS components, of which some may include untrustworthy respectively manipulated semiconductors. E.g., see the discussion about hardware backdoor within the Microsemi ProASIC3 (PA3) A3P250 FPGA back in 2012, a programmable logic mainly used in military high-security applications [27], or the public discussion in case of network products from ZTE and Huawei. Other nowadays well-known examples are the ANT products of the NSA, e.g., hardware or persistent firmware backdoors placed in routers, firewalls and servers, providing hardly detectable hidden entries [28]. While the security issues of COTS in defence applications already have been discussed in NATO back in 2000 [29], this was focused on software products.

Because of the increasing endangerment by COTS hardware, more and more research is done with regard to the identification of malicious behaving COTS, e.g., see [30,31]. Current approaches are rarely applicable in practice, e.g., requiring comprehensive information about the circuit diagram, complex and time-consuming procedures or laboratory-style preconditions for their employment. This may open up possibilities to execute an unrecognized backdoor access, to manipulate systems respectively data or to denial of service of satellite links, C2-systems and even weaponry. Within a NCW scenario this is even more dangerous, because one compromised (trusted) node can have severe effects on the whole network. Compared to free enterprise, this reflects the situation of springboard-attacks, where (worse secured) component suppliers are used for the infiltration of highly-secured companies.

Further implications: Beside the described endangerments for satellites and possible weaknesses and vulnerabilities opened up by COTS products, several other threats must be considered. Because of the limited space of this publication and the broader available coverage in literature, they will only be described briefly. In a full operational NCW scenario, attacks on networks and systems can have severe effects on the capacity to act of a party (e.g., see [32]). This enables even a weaker opponent to gain initiative, destroy the superiority of an enemy and therefore, his force superiority. With a strong dependence on communication networks and computer systems, a comprehensive protection is required. The high flexibility of Software Defined Radio (SDR) compared to conventional radio systems makes it attractive for military applications. On the one hand, systems are available at a reduced rate and can be adapted to changing environmental settings and new requirements, e.g., new waveforms can be integrated easily. On the other hand, moving formerly hard-wired system components to software makes them more vulnerable for attacks and manipulation. As SDR and Cognitive Radio, therefore systems that can be programmed and configured dynamically, will act as an important part of NCW, corresponding endangerments have to be considered (e.g., see [33]).

5. UPCOMING ADVANCES IN COMMUNICATION TECHNOLOGY

NCW enables up-and-coming possibilities to gain information and force superiority by using comprehensive and distributed information and networked sensor and effector grids, even with increasingly smaller armed forces. On the other hand, strongly NCW-based operations are endangered by different threats as shown in Section 4. In the following, upcoming advances in communication technology are analysed, which can be used to build up hardened NCW structures, being capable for utilization within an A2/AD scenario.

The major flaw of NCW is the necessity of reliable communication links. Especially SatCom is of central importance for the successful operation; different upcoming techniques can be used and combined, to improve satellite-based links and to add redundancy in case of a denial of satellite services. Because of the limited space, we will handpick some significant advances in transmission technologies, explaining their capabilities and impact on NCW in more detail.

Satellite-based communication: Military satellite networks have been using SHF- and EHF frequency bands extensively since the 1990s. While only very limited data rates had been available in the beginning, also in higher frequency bands (e.g., see [34]), upcoming advances with regard to technology and waveforms provide the capabilities necessary for NCW. For example, todays Ku-band satellites provide data rates of 5 Mbps and above at almost every location on the globe (excluding Polar Regions); with the deployment of Iridium NEXT beginning this year, Ku- and L-band capabilities are available *worldwide* [35]. Because a wide variety of providers and available systems as well as low equipment costs and small terminals, Ku-band is used increasingly by the military of different countries. But also civilian demand increases steadily, resulting in a high utilization of the available capabilities. The theoretical maximum capacity of Ku-band frequencies is nearly exhausted; e.g., the average gap between Ku-band communication satellites over Europe, North America, south-western Asia and Southeast Asia is about 1.5°, not allowing further positioning of additional Ku-band satellites. On the other hand, the expected demand for SatCom capacity in the 2018 is approx. 232 Gbps, resulting in an equivalent bandwidth of 120 GHz within the Ka-band [36]. Ka-band is more influenced by weather effects because of the higher frequencies compared to Ku-band. Vapour, rain, wet snow, clouds in the troposphere and scintillation effects (absorption of electromagnetic energy by various substances and their transformation into short pulses of visible photons [37]) in the ionosphere effect the transmission path and therefore the achievable data rates, e.g., see [38, 39]. Because of improved transmission quality, this band currently experiences an intense growth (e.g., see [40]) after a decline of available resources in the early 2000s [41]. Having clear sky, Ka-band provides approx. four times higher data rates compared to Ku-band. The crossover, where the data rates of Ka-band drop below Ku-band because of rain effects (400 - 800 Kbps), appears about 5% at wet regions when using a satellite dish of 1.3 m [40]. To compensate weather effects affecting the achievable data rates compared to Ku-band systems, Adaptive Coding and Modulation (ACM) can be used to handle weather-induced fading effects of more than 15 dB [38]; in addition, Ka-band antennas are able to achieve higher antenna gains compared to Ku-band antennas.

Airborne communication nodes: While first systems like the Battlefield Airborne Communications Node (BACN) built by Northrop Grumman already have been used in theatre, their necessity and deployment will increase within NCW scenarios. Besides providing additional bandwidth, they can be used to overcome shortcomings of available network capacity as well as make redundant links available, assuring the functionality of NCW in case of malfunctioning satellites. E.g., BACN can be deployed in unmanned as well as manned aircraft and used as “a forward-deployed airborne communications relay and network-centric enterprise information server” [42].

Terrestrial radio communication: HF-based communications with high data rates are under investigation by military as well as civilian institutions. HF frequencies have been used for wireless communication for decades. Because of the low frequency range from 3 to 30 MHz, these bands are very limited with regard to achievable data rates, typically lying between 75 and 9600 Bd (e.g., see [43]); this is not enough for the link requirements of NCW scenarios. While an extension of STANAG 4539 respectively 5066 at the turn of the millennium implemented data rates of 14400 bps with a bandwidth of 3 kHz [44], Appendix D of the revised standard MIL-STD-188-110C now defines waveforms with bandwidths between 3 and 24 kHz and data rates up to 120 Kbps, using 256-QAM [45]. The new waveforms enable real-time video over HF channels as well as the establishment of ad-hoc IP networks; additional extensions allow data rates up to 240 Kbps [46]. Further studies analyse the transport of time-critical email via HF [47] or the use of iterative equalizers for the improvement of transmission quality and speed (e.g., see [48]). While the capabilities of HF channels are, compared to SatCom links, very limited by nature, modern waveforms and technologies enable IP-based real-time communication opportunities. On the other hand, also satellite resources are very limited, resulting in connections of units with often only about 256 Kbps even this very day. The operating experience in handling these limited links with a comparatively large amount of data and the resulting procedures and protocols are the basis for an efficient integration of modern HF links.

Laser-based communication: Techniques for free-space optical data transmission have been investigated since the 1980s, e.g., see [49]. In the meantime, advanced systems for laser-based communication have reached readiness for start of production [50]. For example, the Lunar Laser Communication Demonstration (LLCD) of NASA in 2013 illustrated the use of a pulsed infrared laser for the communication between earth and moon [51]. Over a distance of 385,000 km, the system provided 622 Mbps downlink and error-free 20 Mbps uplink data rates [52]. LLCD is the basis for a flight optical communications terminal, which is going to be placed in geosynchronous orbit in approx. December 2016. Laser-based communication opens up several outstanding advantages, some of particular interest for the military:

- Highly efficient signal encoding nearby the quantum limit, e.g., by using photon-counting techniques
- Highly effective error-correction in case of a lost laser pulse or tampering by noise
- Very high data rates up to 10 Gbps and later, up to Tbps

- Use of optical links in unregulated parts of the electromagnetic spectrum which are invisible for human eye, hardly detectable (e.g., because of the minimal beam of rays, the optical signal is typically only detectable within a radius of a few 10 m around the receiver [53]) and hardly to interfere by enemies
- Utilization of quantum cryptography for additionally securing the link, e.g., see [54]
- Small terminal sizes

Effects like windblown sand and dust atmosphere can have influence on the transmission quality (e.g., see [55]), but projects like LLCD demonstrate the up-and-coming real-world applicability of this technology.

6. ROBUST NETWORK CENTRIC WARFARE

Based on the identified shortcomings and the up-and-coming capabilities of new technology, requirements for Robust Network Centric Warfare (RNCW) are derived as follows.

1. **Computer Network Defence Capabilities:** As confidentiality, integrity and availability of the network is a key element for utilizing NCW, communication links will remain in the focus for attacks even with hardened links. A strong CNA capability can treat even a weak enemy with favour, therefore enforcing strong CND skills for every NCW-depended actor. Because of that, extensive precautions have to be applied and an immediate (“ real-time”) ability to act must be available when suffering attacks or if network and system anomalies are detected. These are especially *organisational* and *financial* aspects of manning, equipment as well as education and training.
2. **Adaptable protocols:** This requirement is addressing layer 2 to 4 of the ISO model. Protocols for data exchange within NCW systems must be able to adapt to changing link capabilities and connection types, e.g., terrestrial communication and radio-respectively laser-based SatCom. Therefore, they must not only be able to adapt the transmission data rate and to intensify error-correction capabilities on unreliable links, but also to split (multiplex) data through multiple transmission paths and networks, while being able to cope with different delays like jitter and latencies at the same time.
3. **Optimized data/ information exchange requirements:** This aspect is addressing *layer 6 and 7* of the OSI model. Modern services and information requirements necessitate the transmission of huge amounts of data. The basic communication structure must be built on a lightweight system, able to transmit all elementary data of the sensor-, C2- as well as shooter grid over an IPv6 network connection with a data rate of 200 Kbps. This enables scooping out all redundancies of a connection mix; an adequate use of vectorised data sets enables the applicability of all available networks, while additional data can be transmitted within free capacity. Therefore, the data exchange has to adapt in an automated manner to the available connection capabilities. E.g., lowering the quality of un-prioritized video streams can be used to optimize available resources while providing enough bandwidth for critical assets, e.g., UAVs executing an attack or data exchange between units required for third-party targeting.

4. **Hardening of satellite systems:** The endangerments for satellites by ASATs and debris as described in Section 4 underlines the need for further hardening of satellite systems as a critical aspect for the reliability of NCW. Several issues have to be addressed (e.g., see [56]):
   - Hardened circuits (e.g., nuclear hardening with regard to electro-magnetic pulses or Gallium Nitride based solid state power amplifiers)
   - Passive self-defence capabilities, e.g., automated collision-detection and avoidance systems,
   - Active self-defence capabilities, e.g., shoot-back equipment or escort satellites
   - Disperse satellite architectures, for example by smaller satellite payloads
5. **Communication networks:** This requirement is addressing *layer 1*, the physical layer. Because of advantages and disadvantages of radio frequencies of different parts of the electromagnetic spectrum, a mix of various segments of the band must be available for every participant within the NCW system. Upcoming technology enables decreasing terminal sizes and mobile equipment for high frequencies (ultra-small aperture terminals), allowing even the single soldier to have access to different networks at any location on the globe. Platforms like vehicles or ships, as a matter of course, have more space for the installation of communication systems. Based on numerous requirements like the positioning of sensors, weapon systems, minimizing of radar cross sections (RCS), etc., also these systems have only very limited opportunities for the installation of, e.g., stabilized SatCom antennas. For a NCW scenario, extensive data rates are required as shown in Section 3. Based on the steady risk of attacks, weather influence and environmental effects which can influence specific frequency bands respectively links significantly, satellite communication has to be provided by an extensive mix of Ku-, Ka- and SHF-bands. Especially upcoming laser-based systems will be a strong enhancement of secure mobile broadband-connectivity. To be able to provide basic communication in case of a complete denial of space- and aerial based systems, terrestrial systems must *still* be able to sustain basic NCW capabilities. This can be realized by including modern waveforms, which enable data exchange up to 240 Kbps even with HF frequencies [46]. While this is still very limited with regard to satellite links with high data rates, it is enough for elementary data exchange.
6. **Airborne communication-nodes:** UAVs providing communication nodes can be used to provide additional as well as redundant and emergency bandwidth and link capability. While these systems have a very limited dwell time with regard to satellite systems, they are highly flexible and can be used on short notice, strongly enhancing the ability to build-up a resistant and dynamic NCW communication network. These nodes are a mainly a capacity enhancement on the physical layer.
7. **Ability to act autonomously for a short period of time:** One consequence of a possible failure of the communication link is that the individual systems should be able to compensate the loss of communication, at least over a limited time window. This should not be limited to fail-safe operation modes, i.e. where the system keeps its current state (like position, altitude, speed, etc.). Instead, the individual system must continue to be able to perform - at least limited - independent actions to achieve the mission goal(s) (semi-autonomous weapons systems). In addition, the need to be

able to operate locally is also increased by the necessity that forces sometimes have to be able to operate without any communication at all (e.g., within a covert/special operation). For completeness, it should be mentioned that, however, this does not imply "Lethal Autonomous Robotics" (LAR), which are activated once and which - without human intervention - aim for enemies and neutralize them (e.g., see [57] for a controversial paper on lethal autonomous targeting).

Based on these recommendations, resistant, capable and adaptable RNCW can be built-up, establishing the prerequisites for successful operations in future theatres.

7. CONCLUSION

Today's western armed forces are getting increasingly efficient while their sizes are still decreasing. This is possible by achieving information superiority and therefore, to dictate the speed of operation and based on that, utilizing force superiority. This kind of operation requires extensive communication processes and data exchange between all assets and all layers; therefore, a strong network infrastructure is required, enabling the use of NCW. Because of the enhancement of technology, core aspects of NCW are endangered highly nowadays, e.g., communication satellites by attacks of ASATs. Therefore, we first identified severe shortcomings and vulnerabilities of today's NCW and second, investigated up-and-coming technologies that can be used to harden NCW. Based on that, we deduced requirements for RNCW, Robust NCW, to enable the ability to counteract the endangerments of an A2/AD theatre.

ACKNOWLEDGMENT

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Frame-work Programme.

REFERENCES

[1] D. S. Alberts, "Information Age Transformation: Getting to a 21st Century Military (revised)," DTIC Document, Tech. Rep., 2002.

[2] C. Wilson, "Network centric operations: background and oversight issues for congress." DTIC Document, 2007.

[3] Technolytics. Network centric warfare - technology maturity model. [Online]. Available: http://www.directionsmag.com/images/articles/coleman/ncw/ncw3.gif

[4] A. K. Cebrowski and J. J. Garstka, "Network-centric warfare: Its origin and future," in US Naval Institute Proceedings, vol. 124, no. 1, 1998, pp. 28-35.

[5] H. D. Tunnell, "Network-centric warfare and the data-information-knowledgewisdom hierarchy," Military Review, vol. 94, no. 3, p. 43, 2014.

[6] L. Epperson. Satellite communications within the army's win-t architecture. [Online]. Available: http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/492C brief.pdf

[7] U.S. Army CIO/G6, Network Integration Evaluation 15.1 - Technical Architecture. HQDA CIO/G6-AAIC Director, 2013. [Online]. Available: http://ciog6.army.mil/Portals/1/Architecture/NIE_15.1_Technical%20 Architecture_and_Appendices.pdf

[8] The Tacticians Database, “Network-centric warfare.” [Online]. Available: http://tactdb.blogspot.de/2014/06/network-centric-warfare.html

[9] D. S. Alberts, J. J. Garstka, and F. P. Stein, “Network centric warfare: Developing and leveraging information superiority,” DTIC Document, Tech. Rep., 2000.

[10] I. Gordon, J. Matsumura et al., “The army’s role in overcoming anti-access and area denial challenges,” DTIC Document, Tech. Rep., 2013.

[11] “Joint Publication 3-13.1, Electronic Warfare,” Joint, Tech. Rep., 2007.

[12] M. Golling and B. Stelte, „Requirements for a Future EWS - Cyber Defence in the Internet of the Future,“ in Proceedings of the 3rd International Conference on Cyber Conflict (ICCC). IEEE, June 2011, pp. 1-16.

[13] J. Cartwright, “Joint terminology for cyberspace operations,” Joint Chiefs of Staff (JCS) Memorandum, 3Nov, 2010.

[14] National Security Agency. Computer network operations. [Online]. Available: https://www.nsa.gov/careers/career_fields/netopps.shtml

[15] http://archive.defensenews.com. Technical briefing: Anatomy of a bandwidth crunch. [Online]. Available: http://archive.defensenews.com/print/article/20090801/C4ISR02/908010313/Technical-briefing-Anatomy-bandwidth-crunch

[16] Joint Task Force Transformation Initiative, “Managing Information Security Risk,” National Institute of Standards and Technology, Special Publication 800-39, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf last visited on May 21th, 2013.

[17] “Guide for Conducting Risk Assessments,” National Institute of Standards and Technology, Special Publication 800-30, September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf last visited on May 26th, 2013.

[18] G. Marshall. Anti-satellite weapons (asats). [Online]. Available: http://www.space4peace.org/asat/asat.htm

[19] U. N. PUBLICATION, “United nations treaties and principles on outer space (st/space/11),” 2002, sales No. E.02.I.20.

[20] B. Weeden. 2007 chinese anti-satellite test fact sheet. Secure World Foundation. [Online]. Available: http://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf

[21] United States Space Command. Space surveillance. O.J. [Online]. Available: http://www.au.af.mil/au/awc/awcgate/usspc-fs/space.htm

[22] T. Kelso, “Analysis of the 2007 chinese asat test and the impact of its debris on the space environment,” 2007.

[23] K. Tate. Russian satellite crash with chinese asat debris explained (infographic). [Online]. Available: http://www.space.com/20145-russian-satellite-chinese-debris-crash-infographic.html

[24] T. S. Kelso, “Analysis of the iridium 33 - cosmos 2251 collision,” 2009.

[25] T. Kelso. Socrates satellite orbital conjunction reports assessing threatening encounters in space. [Online]. Available: http://celestrak.com/SOCRATES/

[26] K. Ludewigt, T. Riesbeck, T. Baumgärtel, J. Schmitz, A. Graf, and M. Jung, “Mobile and stationary laser weapon demonstrators of rheinmetall waffe munition,” in SPIE Security+ Defence. International Society for Optics and Photonics, 2014, pp. 92 510N-92 510N.

[27] S. Skorobogatov and C. Woods, Breakthrough silicon scanning discovers backdoor in military chip. Springer, 2012.

[28] J. Appelbaum, J. Horchert, and C. Stöcker. Catalog advertises nsa toolbox. SPIEGEL ONLINE 2013. [Online]. Available: http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994-druck.html

[29] NATO Research and Technology Organisation, “Commercial off-the-shelf products in defence applications (the ruthless pursuit of cots),” in Information Systems and Technology Panel (IST-016). NATO, 2000.

[30] S. Wei and M. Potkonjak, “Scalable hardware trojan diagnosis,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 20, no. 6, pp. 1049-1057, 2012.

[31] R. Rad, J. Plusquellic, and M. Tehranipoor, “A sensitivity analysis of power signal methods for detecting hardware trojans under real process and environmental conditions,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 18, no. 12, pp. 1735-1744, 2010.

[32] J. Rantapelkonen, M. Salminen et al., “The fog of cyber defence,” Julkaisusarja 2. Artikkelikokoelma n: o 10, 2013.

[33] A. Banerjee and S. Das, “A review on security threats in cognitive radio,” in Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on, May 2014, pp. 1-5.

[34] Comparison of milsatcom systems. [Online]. Available: http://www.fas.org/spp/military/docops/army/ref text/chap07b.htm

[35] O. Gupta and C. Fish, “Iridium NEXT: A Global access for your sensor needs,” AGU Fall Meeting Abstracts, p. A663, Dec. 2010.

[36] ECC, "The use of the frequency bands 27.5-30.0 GHz and 17.3-20.2 GHz by satellite networks," Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT), Tech. Rep. ECC Report 152, 2010.

[37] Scintillation Materials Research Center. What are scintillation materials? [Online]. Available: http://www.engr.utk.edu/smrc/

[38] J. Petranovich, "Mitigating the effect of weather on ka-band high-capacity satellites," 2012.

[39] A. Dissanayake, "Ka-band propagation modeling for fixed satellite applications," Online Journal of Space Communication, vol. 2, pp. 1-5, 2002.

[40] D. Brunnenmeyer, S. Mills, S. Patel, C. Suarez, and K. Ling-Bing, "Ka and ku operational considerations for military satcom applications," in Military Communications Conference, 2012 - MILCOM 2012, Oct 2012, pp. 1-7.

[41] O.V., "Global analysis of satellite transponder usage and coverage," 2003.

[42] J. Lamar. Northrop grumman airborne communications system wins award for outstanding industry achievement. Northrop Grumman Information Systems. [Online]. Available: http://www.irconnect.com/noc/press/pages/news releases.html?d=184859

[43] M. Uysal and M. Heidarpour, "Cooperative communication techniques for futuregeneration hf radios," Communications Magazine, IEEE, vol. 50, no. 10, pp. 56-63, October 2012.

[44] A. Gillespie and S. Trinder, "Performance characteristics of high data rate hf waveforms," in HF Radio Systems and Techniques, 2000. Eighth International Conference on (IEE Conf. Publ. No. 474), 2000, pp. 335-339.

[45] Department of Defense, "Interoperability and performance standards for data modems," Tech. Rep. Department of Defense Interface Standard, 2011.

[46] M. Jorgenson, R. Johnson, and R. Nelson, "An extension of wideband hf capabilities," in Military Communications Conference, MILCOM 2013 - 2013 IEEE, Nov 2013, pp. 1201-1206.

[47] M. Oezdemir, A. Eliacik, I. Guenes, and A. Sasioglu, "Time-critical e-mail transfer over hf radio," in European Wireless 2014; 20th European Wireless Conference; Proceedings of, May 2014, pp. 1-6.

[48] M. Elgenedy, E. Sourour, and M. Nafie, "Iterative mmse-dfe equalizer for the high data rates hf waveforms in the hf channel," in Signals, Systems and Computers, 2013 Asilomar Conference on, Nov 2013, pp. 1243-1247.

[49] V. Rampal, "Blue green lasers and their military potential," Defence Science Journal, vol. 33, no. 2, pp. 183-193, 1983.

[50] S. Magnuson. (2013) Game-changing laser communications ready for fielding, vendors say. National Defense Magazine. [Online]. Available: http://www.nationaldefensemagazine.org/archive/2013/January/Pages/Game-ChangingLaserCommunicationsReadyForFielding,VendorsSay.aspx?PF=1

[51] B. L. Edwards, D. Israel, K. Wilson, J. Moores, and A. Fletcher, "Overview of the laser communications relay demonstration project." [Online]. Available: http://www.spaceops2012.org/proceedings/documents/id1261897-paper-001.pdf

[52] J. Buck. Nasa laser communication system sets record with data transmissions to and from moon. [Online]. Available: http://www.nasa.gov/press/2013/october/nasa-laser-communication-system-sets-record-with-data-transmissions-to-and-from/

[53] D. Giggenbach, "Mobile optical high-speed data links with small terminals," in SPIE Europe Security+ Defence. International Society for Optics and Photonics, 2009, pp. 74 800I-74 800I.

[54] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. Lamoreuax, G. Morgan, J. E. Nordholt, and C. G. Peterson, "Quantum cryptography for secure satellite communications," in Aerospace Conference Proceedings, 2000 IEEE, vol. 1. IEEE, 2000, pp. 191-200.

[55] Y. Ruike, H. Xiange, H. Yue, and S. Zhongyu, "Propagation characteristics of infrared pulse waves through windblown sand and dust atmosphere," International Journal of Infrared and Millimeter Waves, vol. 28, no. 2, pp. 181-189, 2007. [Online]. Available: http://dx.doi.org/10.1007/s10762-006-9186-4

[56] Harrison, Todd, "The Future of MILSATCOM," Center for Strategic and Budgetary Assessments, CSBA Study, July 2013.

[57] N. Sharkey, "Saying `no!' to lethal autonomous targeting," Journal of Military Ethics, vol. 9, no. 4, pp. 369-383, 2010.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Supporting Sense-Making and Decision-Making Through Time Evolution Analysis of Open Sources*

Andrea Balboni
Interdepartment Research Center on Security
University of Modena and Reggio Emilia
Modena, Italy
andrea.balboni@unimore.it

Michele Colajanni
Interdepartment Research Center on Security
University of Modena and Reggio Emilia
Modena, Italy
michele.colajanni@unimore.it

Mirco Marchetti
Interdepartment Research Center on Security
University of Modena and Reggio Emilia
Modena, Italy
mirco.marchetti@unimore.it

Andrea Melegari
Expert System s.p.a.
Modena, Italy
amelegari@expertsystem.com

Abstract: Modern societies produce a huge amount of open source information that is often published on the Web in a natural language form. The impossibility of reading all these documents is paving the way to semantic-based technologies that are able to extract from unstructured documents relevant information for analysts. Most solutions extract uncorrelated pieces of information from individual documents; few of them create links among related documents and, to the best of our knowledge, no technology focuses on the time evolution of relations among entities. We propose a novel approach for managing, querying and visualizing temporal knowledge extracted from unstructured documents that can open the way to novel forms of sense-making and decision-making processes. We leverage state-of-the-art natural language processing engines for the semantic analysis of textual data sources to build a *temporal graph database* that highlights relationships among entities belonging to different documents and time frames. Moreover, we introduce the concept of *temporal graph query* that analysts can use to identify all the relationships of an entity and to visualize their evolution over time. This process enables the application of statistical algorithms that can be oriented to the automatic analysis of anomalies, state change detection, forecasting. Preliminary results demonstrate that the representation of the evolution of entities and relationships allows an analyst to highlight relevant events among the large amount of open source documents.

Keywords: *open sources, semantic analysis, temporal query, sense-making, decision-making*

* This project has been funded with support from the European Commission. Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

1. INTRODUCTION

Decision-making and sense-making processes take advantage of actionable intelligence gathered from any available information source. The increasing volume of information that analysts can access from the Web augments the importance of *Open-Source Intelligence* (OSINT) (Glassman & Kang, 2012). It is impossible for humans to manage the huge amount of information published on a daily basis as unstructured text documents, possibly written in many different languages. Hence, analysts often rely on software for the semantic analysis of natural language (Baldini, Neri, & Pettoni, 2007) (Neri, Aliprandi, & Camillo, 2011) (Steele, 2007) (Richard A. Best, 2008) (Best, 2008). Modern semantic technologies support OSINT through several features, such as topic detection, categorization and mining of entities and relationships. However, these operations are mostly oriented towards *intra-document relationships* and do not take into account *inter-document relationships* and their dynamics in time.

In this paper, we propose a novel scalable architecture for processing the output produced by semantic engines for natural text analysis and that guarantees the following novel features:

- Detection of relationships among entities that occur in the same document *(intra-document relationships)*;
- Detection of relationships among entities that occur in different documents *(inter-document relationships)*;
- Analysis of how entities and relationships evolve over time;
- Extraction of quantitative numerical data that can be analyzed through statistical algorithms.

We have designed and implemented a prototype that fully implements the processing architecture proposed in this paper and that can execute expressive queries over huge volumes of documents to easily extract information related to entities and their relationships and describe how they evolve over time. This work poses the basis for novel forms of sense-making and decision-making supported by algorithms for graph analysis and by statistical algorithms for the analysis of time series, that can be tailored to anomaly detection, state change detection and forecasting.

The remainder of the paper is organized as follows. Section 2 illustrates the main components of the architecture and the foundations of the semantics analysis technologies employed. Sections 3 and 4 describe the most important components of the proposed architecture: the parser that processes the output of the semantic engine, the *temporal graph database* that organizes intra- and inter-document relationships, the parallel query operations executed among the relevant graph databases. Section 5 presents experimental results obtained through a prototype. Section 6 discusses related work. Section 7 contains concluding remarks and some directions for future work.

2. ARCHITECTURE DESIGN

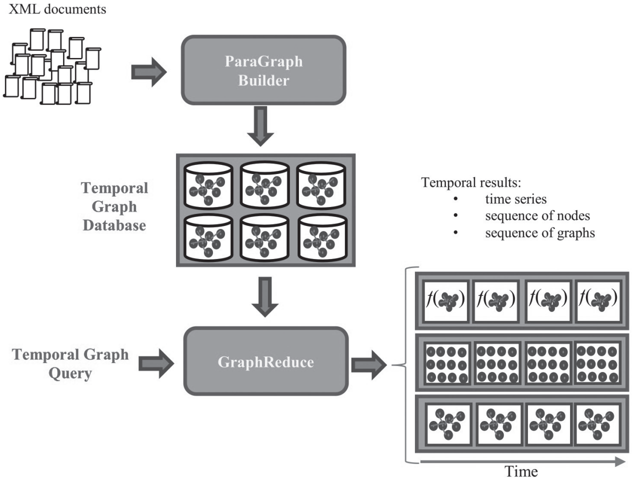
The semantic analysis of natural language is a fundamental enabler for any text analytics methodology. However, traditional engines for semantic analysis suffer some drawbacks that become more evident as the number of documents to analyze increases. For example, after processing large corpora of documents, a semantic engine produces a huge volume of annotated documents (usually in XML format) that needs further processing for scalable storage, indexing and querying. Moreover, since annotated documents are not mutually linked, it is difficult to identify all the facts that involve a given entity and that are described in several different documents.

These motivations induced us to design a novel processing architecture for supporting analysts in storing, connecting and querying all the information produced by engines for semantic analysis. The proposed architecture is based on three main design principles enlisted below:

- The system must be inherently scalable, and designed to run on modern hardware leveraging multicore architectures, distributed file systems and parallel processing of huge amounts of data.
- The second design principle is the focus on relationships among entities across large document sets, rather than on a single document. Indeed, one of our main goals is to establish inter-document relationships, thus allowing analysts to identify all the facts/ events involving the same entities or linked by the same relationships. To this end, the information contained in the semantically annotated text documents (produced by semantic engines) are modelled as graphs that contain entities, their relationships and other relevant elements providing information on the context. This design choice has a twofold advantage: it enables the creation of inter-document relationships by connecting graphs related to different documents; it allows us to leverage the state-of-the-art on graph analytics, management and visualization algorithms (Nisar, Fard, & Miller, 2013) (Nguyen, Lenharth, & Pingali, 2013).
- The third design principle is the introduction of the notion of time. With a temporal reference, it is possible to perform novel forms of analysis that show how relationships among entities have evolved, thus giving analysts some insights about the phenomena of interest.

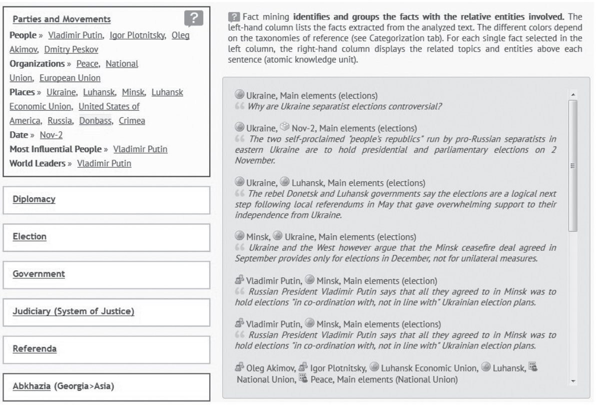
The proposed architecture also supports the extraction of time series that can be analyzed through several statistical algorithms with the aim of eliminating noise (Tosi, Casolari, & Colajanni, 2013), identifying anomalies (Chandola, Banerjee, & Kumar, 2009) and correlations among time series (Esling & Agon, 2012) (Hamilton, 1994) and forecasting their evolution (Brockwell & Davis, 2002). The main components of the processing architecture and its information flow are illustrated in Figure 1.

FIGURE 1: INFORMATION FLOW AND MAIN COMPONENTS OF THE PROPOSED ARCHITECTURE.



Annotated XML documents produced by a semantic engine represent the input of the proposed processing architecture. A semantic engine produces structured information according to different *information channels*. The semantic engine used by our prototype is Cogito Intelligence API (Expert System s.p.a., 2014) which provides 13 information channels that rely on specific taxonomies. The *Fact Mining* category includes specific taxonomies such as *Intelligence, Cyber, Crime* and *Geography*. A *fact* is a collection of entities contained in parts of text (e.g. sentences) categorized according to a set of predefined *domains* and may be described by one or more *topics* (in the *domain*). Focused analyses can be executed by evaluating entities and their relationships in a context involving domains and topics of interest. Figure 2 shows the output of the Fact Mining engine on open source content (http://www.bbc.com/news/world-europe-29831028) obtained with the free web demo of Cogito Intelligence API (Expert System s.p.a., 2015).

FIGURE 2: DEMO WEB APPLICATION OF THE COGITO INTELLIGENCE API.



Parties and Movements

People » Vladimir Putin, Igor Plotnitsky, Oleg Akimov, Dmitry Peskov
Organizations » Peace, National Union, European Union
Places » Ukraine, Luhansk, Minsk, Luhansk Economic Union, United States of America, Russia, Donbass, Crimea
Date » Nov-2
Most Influential People » Vladimir Putin
World Leaders » Vladimir Putin

Diplomacy

Election

Government

Judiciary (System of Justice)

Referenda

Abkhazia (Georgia>Asia)

? Fact mining **identifies and groups the facts with the relative entities involved.** The left-hand column lists the facts extracted from the analyzed text. The different colors depend on the taxonomies of reference (see Categorization tab). For each single fact selected in the left column, the right-hand column displays the related topics and entities above each sentence (atomic knowledge unit).

Ukraine, Main elements (elections)
Why are Ukraine separatist elections controversial?

Ukraine, Nov-2, Main elements (elections)
The two self-proclaimed "people's republics" run by pro-Russian separatists in eastern Ukraine are to hold presidential and parliamentary elections on 2 November.

Ukraine, Luhansk, Main elements (elections)
The rebel Donetsk and Luhansk governments say the elections are a logical next step following local referendums in May that gave overwhelming support to their independence from Ukraine.

Minsk, Ukraine, Main elements (elections)
Ukraine and the West however argue that the Minsk ceasefire deal agreed in September provides only for elections in December, not for unilateral measures.

Vladimir Putin, Minsk, Main elements (election)
Russian President Vladimir Putin says that all they agreed to in Minsk was to hold elections "in co-ordination with, not in line with" Ukrainian election plans.

Vladimir Putin, Minsk, Main elements (elections)
Russian President Vladimir Putin says that all they agreed to in Minsk was to hold elections "in co-ordination with, not in line with" Ukrainian election plans.

Oleg Akimov, Igor Plotnitsky, Luhansk Economic Union, Luhansk, National Union, Peace, Main elements (National Union)

The *ParaGraph Builder* component analyzes each annotated document, extracts the intra-document graph and populates the *Temporal Graph Database* by merging intra-document graphs into dynamic inter-document graphs. The Temporal Graph Database represents the main information repository that analysts can query to extract useful information. Operations of the ParaGraph builder are described in Section 3. Knowledge extraction is performed through *Temporal Graph Queries* that analysts can submit to another key component called GraphReduce. *GraphReduce* interprets all the temporal queries and processes dynamic inter-document graphs that are stored in the Temporal Graph Database to produce temporal results. Depending on the query submitted by the analysts, temporal results can take three main forms:

- If a function is used to extract a numerical value from graphs, the result is a time series in which each element represents the numerical value computed on the resulting graph in the corresponding timeframe;
- If the temporal query considers entities and not relationships (e.g., by asking for all the entities that are related to Al-Qaeda), then the temporal results are a sequence of sets of entities, that are represented by nodes of a graph;
- If the temporal query aims to represent how entities and their relationships evolve over time, then the temporal results are a sequence of graphs.

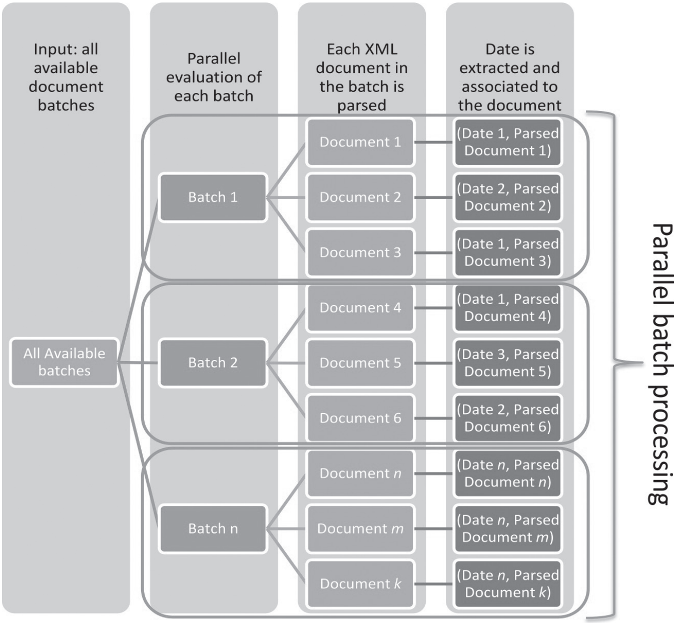
Operations of GraphReduce are described in Section 4.

3. PARAGRAPH BUILDER

The ParaGraph builder analyzes the annotated XML documents produced by the semantic engine and populates the Temporal Graph Database in a two-stage processing pipeline:

- parallel document parsing;
- graph database population.

FIGURE 3: PARALLEL DOCUMENT PARSING PIPELINE OF THE PARA GRAPH BUILDER

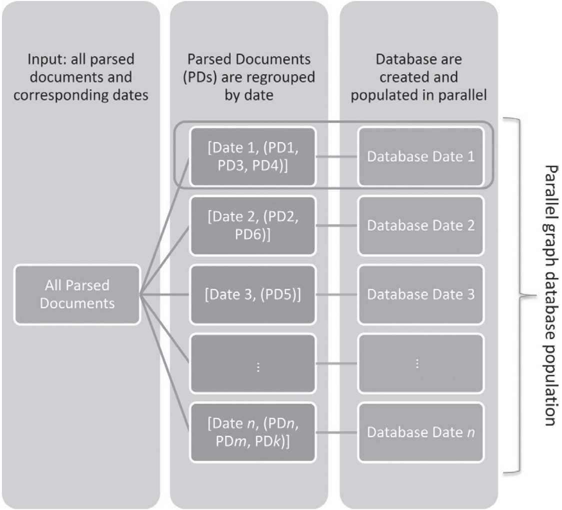

Input: all available document batches
Parallel evaluation of each batch
Each XML document in the batch is parsed
Date is extracted and associated to the document
All Available batches
Batch 1
Batch 2
Batch n
Document 1
Document 2
Document 3
Document 4
Document 5
Document 6
Document n
Document m
Document k
(Date 1, Parsed Document 1)
(Date 2, Parsed Document 2)
(Date 1, Parsed Document 3)
(Date 1, Parsed Document 4)
(Date 3, Parsed Document 5)
(Date 2, Parsed Document 6)
(Date n, Parsed Document n)
(Date n, Parsed Document m)
(Date n, Parsed Document k)
Parallel batch processing

The parallel document parsing pipeline is depicted in Figure 3. In this phase annotated document batches are processed in parallel by the ParaGraph builder, thus guaranteeing high scalability and efficient use of resources in multicore computational architectures.

For each parsed document (PD) in the input batch, the ParaGraph Builder outputs the intra-document graph containing a temporal reference and all the entities and relationships that belong to the Intelligence, Crime and Geography information channels. Any analysis of the evolution of facts, entities and relationships over time relies on the ability to determine the timeframe. This activity can be performed reliably for certain classes of documents, such as news published by on-line newspapers and press agencies on the Web or as RSS feeds. Precise dating of other classes of documents is still an open research area. Each parsed document is associated to (a) the source document, (b) *facts* identified by the semantic analyzer, (c) *topics* and *entities* associated to facts. Parsed documents represent the input for the second processing stage represented in Figure 4. All intra-document graphs whose time reference belong to the same timeframe (e.g. the same calendar day) are aggregated to form a group. Each group contains intra-document graphs that the ParaGraph Builder stores within the same graph database. If a Temporal Graph Database for the timeframe corresponding to a group already exists, the ParaGraph Builder incrementally adds all the new inter-document graphs to the existing group. In particular, it fuses intra-document graph with the other graphs that contain the same entities, thus creating an inter-document graph whose entities and relationships are gathered from many different documents. If the semantic engine is able to recognize that the same entity appears in different documents, even if with different names, all the instances of the same entity will be fused together. On the other hand, if a graph database for a target timeframe does not exist, the ParaGraph builder creates a new graph database and populates it by inserting all the intra-document graphs contained in the group. All graph databases are populated in parallel, thus ensuring scalability and efficient resource usage on modern multicore architectures and distributed file systems. The set of all the graph databases that store inter-document graphs related to all timeframes forms the Temporal Graph Database and represents the primary knowledge base of the proposed processing architecture.

The graph database used in or prototype implementation is Neo4j (Holzschuher & Peinl, 2013), characterized by a large user community, high performance and scalability, and the support for a powerful graph query language. The Temporal Graph Database is a collection of instances of Neo4j databases. Each graph database instance can be queried independently.

FIGURE 4: PARALLEL GRAPH DATABASE POPULATION PIPELINE OF THE PARAGRAPH BUILDER.

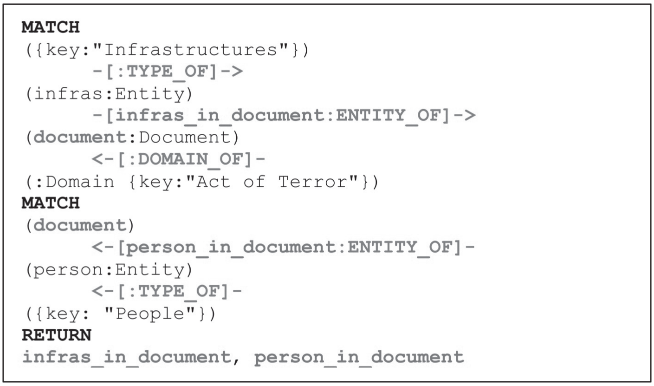

Input: all parsed documents and corresponding dates
Parsed Documents (PDs) are regrouped by date
Database are created and populated in parallel
All Parsed Documents
[Date 1, (PD1, PD3, PD4)]
[Date 2, (PD2, PD6)]
[Date 3, (PD5)]
⋮
[Date *n*, (PD*n*, PD*m*, PD*k*)]
Database Date 1
Database Date 2
Database Date 3
⋮
Database Date *n*
Parallel graph database population

4. GRAPHREDUCE

GraphReduce provides the interface between analysts and all the data stored in the Temporal Graph Database. To extract information from the Temporal Graph Database, the analyst interacts with GraphReduce by issuing queries that are executed in parallel among all the relevant graph databases. When all the parallel queries terminate, GraphReduce collects the partial results and merges them into a single result that is presented to the analyst.

Graph databases are queried through specific query languages that differ from standard query languages for relational databases. In particular, query languages for graph databases focus on the relationships among entities, and are able to express the concept of direct and indirect connections among entities. Graph queries on Neo4j are expressed via the Cypher (Holzschuher & Peinl, 2013) language. An example of query expressed in Cypher is given in Figure 5.

FIGURE 5: EXAMPLE OF GRAPH QUERY EXPRESSED IN CYPHER QUERY LANGUAGE.



```
MATCH
({key:"Infrastructures"})
      -[:TYPE_OF]->
(infras:Entity)
      -[infras_in_document:ENTITY_OF]->
(document:Document)
      <-[:DOMAIN_OF]-
(:Domain {key:"Act of Terror"})
MATCH
(document)
      <-[person_in_document:ENTITY_OF]-
(person:Entity)
      <-[:TYPE_OF]-
({key: "People"})
RETURN
infras_in_document, person_in_document
```

This query runs over a graph database and returns a sub-graph that represents all the entities of type “People” and “Infrastructures” that participate in facts belonging to the domain “Act of Terror”. It comprises two sub-queries, each introduced by the “MATCH” keyword. The first sub-query identifies all the documents that satisfy two properties: 1) they are connected through a relationship of type “DOMAIN_OF” to the domain “Act of Terror”; 2) they are connected through relationships of type “ENTITY_OF” to entities whose type is “Infrastructures”. We can see from Figure 5 that relationships are represented by arrows and are described by couples “NAME:TYPE” within square brackets (-[NAME:TYPE]->). The name is not mandatory, but can be used to reference the same relationship or the same entity in other parts of the query. As an example, all documents that satisfy the two constraints expressed in the first sub-query are given the name “document”, while all relationships that connect an entity of type “Infrastructure” to a document are referenced by the name “infras_in_document”. The second sub-query expresses a further constraint by selecting only documents that contain entities of type “People”. The relationships returned in the resulting sub-graph are named “person_in_document”.

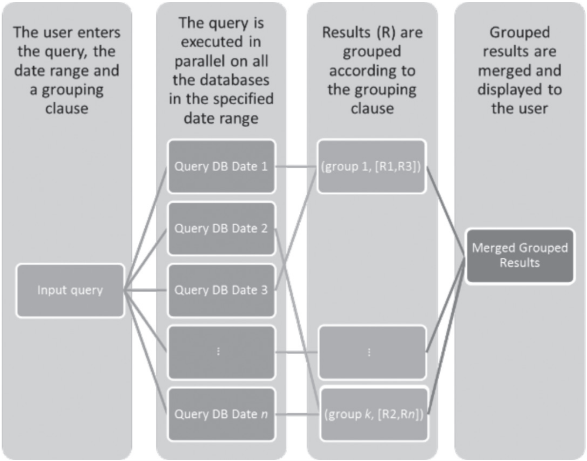
After selecting a subset of entities and relationships through “MATCH” keywords, Neo4j produces an output that contains all the relationships named “infras_in_document” and “person_in_document”, as prescribed by the last part of the query introduced by the keyword “RETURN”. Since a relationship implicitly includes the connected entities, the result produced by Neo4j is a graph.

While Cypher is a powerful query language, it lacks specific keywords to express temporal constraints. Hence, we defined a new class of queries, called *Temporal Graph Queries*, that enrich Cypher by introducing four new keywords that express temporal constraints. Temporal Graph Queries are represented via standard JSON (JavaScript Object Notation) data structures (Ihrig, 2013). A temporal query includes four different elements:

- The first element, introduced by the keyword "query", represents a Cypher graph query. In principle, it could be expressed in any other language used to query graphs, such as the Gremlin query language (Tausch, Philippsen, & Adersberger, 2011);
- The second and third elements are the *start date* and the *end date* that correspond to the keywords "sdate" and "edate", respectively. These two keywords define the timeframe over which the query has to be executed;
- The fourth element is the *grouping clause*, expressed by the "groupClause" keyword. For example, a grouping clause "byMonth" means that all the temporal results are grouped on a monthly basis. If a selected timeframe consists of twenty-four months, the temporal results are grouped in twenty-four different graphs, each representing the data related to one calendar month.

A query result is always a series of homogeneous "objects" that can be graphs, sets of entities or numerical values. The particular format depends on the analysis focus.

FIGURE 6: MAIN PROCESSING PHASES OF GRAPHREDUCE.


The user enters the query, the date range and a grouping clause
The query is executed in parallel on all the databases in the specified date range
Results (R) are grouped according to the grouping clause
Grouped results are merged and displayed to the user
Input query
Query DB Date 1
Query DB Date 2
Query DB Date 3
⋮
Query DB Date n
(group 1, [R1,R3])
⋮
(group k, [R2,Rn])
Merged Grouped Results

Graphs are best suited to analyze how the relationships among entities evolve over time; sets of entities are good at identifying which entities (e.g., people, infrastructures, organizations) are mentioned in facts belonging to specific domains; numerical values can be used to build time series that represent the evolution over time of any metric that can be extracted from data.

Temporal queries are received by GraphReduce that executes them efficiently over all the graph databases that belong to the Temporal Graph Database.

Figure 6 shows the main processing steps performed by GraphReduce while executing a temporal graph query. Start and end dates included in the temporal query are used to select only the subset of graph databases that is relevant for the query. The Cypher query included in the temporal query is executed in parallel over all the relevant graph databases. This design choice ensures high scalability and performance.

Since the set of relevant databases depends only on the timeframe identified in the temporal query, the execution time of the query does not depend on the overall size of the Temporal Graph Database. As the result, queries are very efficient because the size of each graph database group is relatively small (an experimental evaluation of the performance and hardware requirements of the prototype is proposed in Section 5).

Temporal queries expressed over large timeframes require the parallel execution of the same query over a high number of graph databases. However, each graph database is queried independently, and the time required to execute the query over all the graph database is limited by the number of queries that can be executed concurrently. Since the proposed architecture is highly parallelized, it is possible to improve performance by leveraging modern distributed file systems and an appropriate number of processing nodes.

After completion of all the parallel graph queries, GraphReduce collects all results and groups them according the grouping clause expressed in the temporal query. Grouped results are merged in an ordered sequence of objects that is presented to the analyst.

5. EXPERIMENTAL EVALUATION

The experimental testbed used to evaluate the performance of our prototype consists of three main elements: two processing nodes, both equipped with two Intel Xeon E5_2620 CPUs, each with 6 physical cores and support for hyperthread technology, for a total of 24 logical processors, and 16 GB of RAM; a storage node composed of a Storage Area Network (SAN) Fujitsu Eternus DX80 S2 including 36 SAS hard drives, with a rotational speed of 15k rpm and 600 GBytes of size. The logical volume used to store the Temporal Graph Database contains 8 physical disks in a high performance RAID 1+0 configuration, for a total of 2.1 TB storage space.

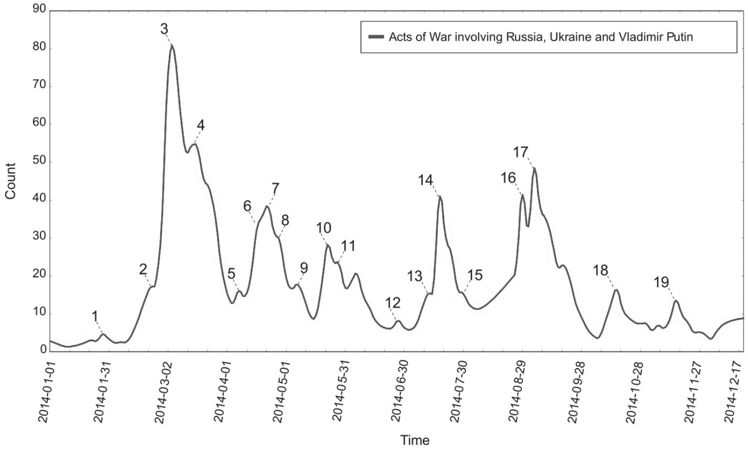
The operating system installed on the processing nodes is Debian Jessie GNU/Linux. The graph databases are implemented through Neo4j version 2.1.2. The ParaGraph builder and GraphReduce components were developed in the Scala programming language (Odersky, Spoon, & Venners, 2008) and leverage the Apache Spark (Zaharia, Chowdhury, Franklin, Shenker, & Stoica, 2010) in-memory map reduce framework (Dean & Ghemawat, 2008).

We tested the prototype by processing 500K annotated documents produced by Cogito. Source documents in natural language are represented by news that can be freely downloaded from the websites and RSS feeds of the major international newspapers and press agencies. These documents were downloaded daily for 18 months. The resulting Temporal Graph Database has a size of 18 GBytes and includes 1835 distinct databases having 676403 distinct entities. Analyzing all the documents and rebuilding the Temporal Graph Database from scratch requires about 60 minutes. All the results presented in this section rely on this dataset.

We present three use cases that demonstrate some of the most important features of the proposed system, and its support for analysis. As a first use case, we consider the ability of our system to create timelines that reflect the popularity of a particular fact in the news. As an example, Figure 7 contains a timeline representing the amount of news that contain facts belonging to the domains “War” and “War Crime” involving Russia, Ukraine and Vladimir Putin. The temporal query considers all the news created in year 2014 with a granularity of three days. To eliminate noise and to provide a better visualization, the system applies an exponential moving average filter (Holt, 2004).

In order to appreciate the capability of the system to produce a significant time series that captures the most important facts related to a given query, we use as our ground truth the list of facts that are included in the timeline of the Russia-Ukraine crises published by the BBC (BBC News Europe, 2015). Selected events from the BBC timeline are associated to numbers (from 1 to 19) which correspond to specific points in the time series. The associations between facts and numbers is given in Table 1. Figure 7 highlights that relevant events are associated to local maximums and abrupt changes in the slope of the timeline. Hence, an analyst can issue a query to pinpoint when relevant facts occurred, and then focus on the analysis of facts that have occurred at specific times.

FIGURE 7: TIME SERIES REPRESENTING THE NUMBER OF NEWS RELATED TO ACTS OF WAR BETWEEN RUSSIA AND UKRAINE INVOLVING VLADIMIR PUTIN OVER THE YEAR 2014.



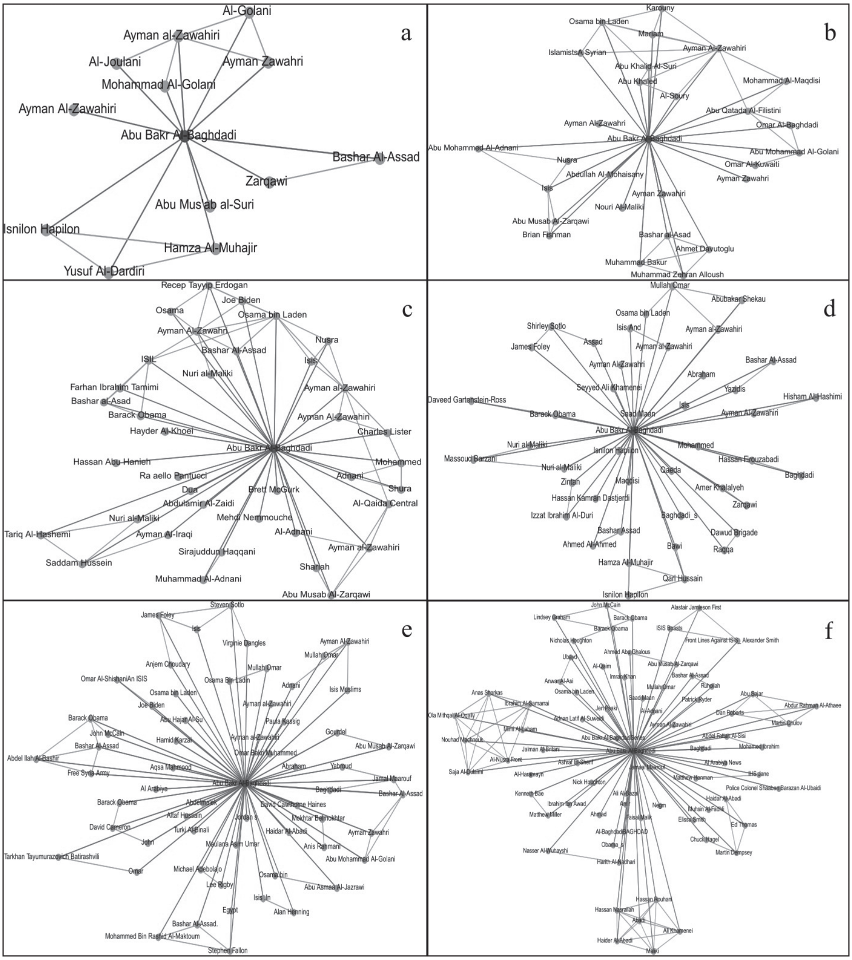
The preceding query provides an example of a realistic question that could be expressed by an analyst interested in studying the evolution of the crisis between Russia and Ukraine, and of the role of Vladimir Putin. We stress that a similar query cannot be easily expressed through other tools commonly used by analysts. Indeed, an equivalent keyword-based search would be much less effective and would return an endless list of documents ordered by custom ranking algorithms (in a black box approach) that not necessarily reflect the expectations of the analyst. The prototype is able to execute the query and generate the time series in less than 3 minutes on a platform with medium-low computational power. Using a more powerful architecture, we can offer to an analyst the ability to issue queries and visualize the results interactively.

TABLE 1: RELEVANT EVENTS RELATED TO THE RUSSIA-UKRAINE CRISIS PUBLISHED BY THE BBC.

#	Fact
1	Prime Minister Mykola Azarov resigns and parliament annuls the anti-protest law. Parliament passes amnesty bill but opposition rejects conditions.
2	Kiev sees its worst day of violence for almost 70 years. At least 88 people are killed in 48 hours. Video shows uniformed snipers firing at protesters holding makeshift shields.
3	Russia's parliament approves President Vladimir Putin's request to use force in Ukraine to protect Russian interests.
4	President Putin signs a bill to absorb Crimea into the Russian Federation.
5	Protesters occupy government buildings in the east Ukrainian cities of Donetsk, Luhansk and Kharkiv, calling for a referendum on independence. Ukrainian authorities regain control of Kharkiv government buildings the next day.
6	Ukraine's acting President, Olexander Turchynov, announces the start of an "anti-terrorist operation" against pro-Russian separatists. It quickly stalls.
7	Russia, Ukraine, the US and the EU say they have agreed at talks in Geneva on steps to "de-escalate" the crisis in eastern Ukraine. Three people are killed when Ukrainian security forces fend off a raid on a base in Mariupol - the first violent deaths in the east.
8	Ukraine's acting president orders the relaunch of military operations against pro-Russian militants in the east.
9	Clashes in the Black Sea city of Odessa, leave 42 people dead, most of them pro-Russian activists. Most die when they are trapped in a burning building.
10	News coverage about upcoming elections in Ukraine
11	Ukraine elects Petro Poroshenko as president in an election not held in much of the east.
12	Russia's parliament cancels a parliamentary resolution authorising the use of Russian forces in Ukraine.
13	Rebels abandon their command centre at Sloviansk in the face of a government offensive.
14	Malaysia Airlines flight MH17 from Amsterdam is shot down near the village of Grabove in rebel-held territory, with the loss of 298 lives.
15	The EU and US announce new sanctions against Russia.
16	Rebel leader Alexander Zakharchenko says there are 3-4,000 Russian civilians in rebel ranks as the separatists open up a front on the Sea of Azov and capture Novoazovsk.
17	Ukraine and pro-Russian rebels sign a truce in Minsk.
18	President Putin orders thousands of troops stationed near the Ukrainian border to return to their bases.
19	Nato commander Gen Philip Breedlove says Russian military equipment and Russian combat troops have been seen entering Ukraine in columns over several days.

Another interesting example is the study of the social network of a given entity. Figure 8 shows the results of a temporal query that aims at identifying the connections between Abu Bakr Al-Baghdadi and all other persons that are involved in the same facts in the year 2014.

FIGURE 8: SERIES OF GRAPHS REPRESENTING THE EVOLUTION OF THE SOCIAL NETWORK OF ABU BAKR AL-BAGHDADI FOR THE YEAR 2014. EACH GRAPH REPRESENTS TWO MONTHS.



The temporal query groups results on a bimonthly basis, therefore Figure 8 includes six graphs representing the social network of Abu Bakr Al-Baghdadi in different periods of the year (Figure 8.a refers to January and February, 8.b to March and April, and so on). Even without applying complex graph analysis algorithms, it is evident how the social network grows over time. An analyst could infer that the person under analysis has a growing importance, and there are an increasing number of contacts that could be further explored. A quantitative analysis of the numbers of vertexes and edges of each sub-graph that supports this conclusion is represented in Table 2.

TABLE 2: NUMBER OF VERTEXES AND EDGES OF GRAPHS SHOWN IN FIGURE 8.

	Number of direct connections (degree) of Abu Bakr Al-Baghdadi	Total number of connections (edges) of the social network
January-February (a)	12	21
March-April (b)	27	60
May-June (c)	37	79
July-August (d)	43	64
September-October (e)	60	95
November-December (f)	72	128

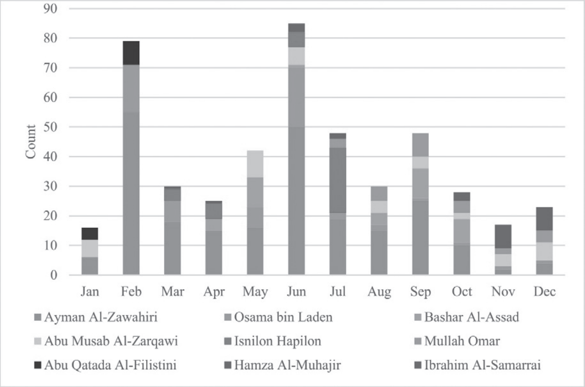
Graphs also highlight different types of relationships. Blue edges identify direct contacts between Abu Bakr Al-Baghdadi and other persons that participate to the same facts, while edges in grey represent direct contacts among persons that are related to Abu Bakr Al-Baghdadi. This representation helps analysts in identifying groups of persons that are directly related to the target node (Abu Bakr Al-Baghdadi) and also triadic closures.

Finally, we present a different graphical representation that can aid analysts in highlighting the relationships between a person and her most active contacts. Figure 9 shows a stacked histogram that represents the number of facts in which Abu Bakr Al-Baghdadi was mentioned together with his top 9 contacts.

From this representation, it is possible to differentiate easily between:

- stable contacts, that are present in all months (such as Ayman Al-Zawahiri);
- recurrent contacts, that are not always present but that appear throughout the year (such Abu Musab Al-Zarqawi);
- old contacts, that were stable or recurrent but stop appearing at a certain point in time (such as Abu Qata Al-Filistini);
- new contacts, that were not present in the past and start appearing at some point in time (such as Ibrahim Al-Samarrai).

FIGURE 9: EVOLUTION OF THE NUMBER OF CO-OCCURRENCES BETWEEN ABU BAKR AL-BAGHDADI AND HIS TOP 9 CONTACTS.



Moreover, by considering the height of the segment associated to a person, it is possible to highlight trends that represent the importance of that person. As an example, from Figure 9 it is possible to conclude that the number of co-occurrences between Abu Bakr Al-Baghdadi and Mullah Omar, that started appearing in July 2014, are stable, while co-occurrences with Ayman Al-Zawairi show a declining trend starting from June 2014.

6. RELATED WORK

This work leverages state of the art engines for semantic (Expert System s.p.a., 2014) analysis and graph analytics (Nguyen, Lenharth, & Pingali, 2013) to extract useful knowledge from textual documents and allow analysts to express complex queries.

Several works in the literature focus on extracting information from documents in natural language. A large corpus of papers refers to sentiment analysis and opinion mining (Pang & Lee, 2008) applied to several information sources. In particular, most of the previous work focus on microblogging platforms (Pak & Paroubek, 2010) (Agarwal, Xie, Vovsha, Rambow, & Passonneau, 2011) (Deng, et al., 2013) and larger documents such as news and blogs (Godbole, Srinivasaiah, & Skiena, 2011).

Our paper relates more closely to works that analyze natural language documents to mine facts and topics and entities (Aggarwal & Zhai, 2012). In particular, several papers focus on the extraction of entities and facts from news articles (Etzioni, et al., 2005) (Pa_ca, Lin, Bigham, Lifchits, & Jain, 2006), but without creating inter-document links. Another class of papers focuses on creating clusters of linked documents that likely refer to the same topics or facts (Wanner, et al., 2014). However, these papers do not consider the notion of time and do not extract facts and entities from clustered documents.

A step further is taken by STORIES (Berendt & Subasic, 2009), a system that clusters documents that contain the same keywords and links them together according to their publication time. However, this work do not leverage state-of-the-art semantic analysis, hence it is not able to extract entities, facts and their relationships from documents. Moreover, it does not support the execution of complex temporal queries similar to those presented in Section 5.

To the best of our knowledge, this is the first paper that presents a processing architecture and a prototype able to analyze large corpora of documents in a scalable way, leverage state-of-the-art engines for semantic analysis, create inter-document links, consider the dimension of time, support complex temporal graph queries and produce several different types of outputs.

7. CONCLUSION

This paper proposes a novel computational architecture that can support analysts in decision-making and sense-making processes, as well as in OSINT activities. The proposed approach takes as its input documents processed by state-of-the-art semantic engines and augments this information by automatically creating links across different documents and by introducing the notion of time. This framework enables analysts to execute complex queries over large corpora of documents and to highlight how entities, relationships and metrics of interest vary over time. The proposed approach is scalable by design, and experimental results obtained through a prototype demonstrate that the time needed to execute queries is compatible with interactive data analysis. Future work will strive to integrate algorithms for automatic time series analysis in the proposed architecture, thus embedding in the system the ability to identify anomalies, correlations and to produce forecasts for the temporal data of interest.

ACKNOWLEDGMENT

The work presented in this paper has been founded by the EU project "SNAPSHOT: *a Social Network Analysis Platform for the Support of European and Homeland Threat Prevention and Strategies"*. Grant agreement CIPS 4000003757.

REFERENCES

Agarwal, A., Xie, B., Vovsha, I., Rambow, O., & Passonneau, R. (2011). Sentiment Analysis of Twitter Data. *Proceedings of the Workshop on Language in Social Media (LSM 2011)* (pp. 30-38). Portland, OR, USA: Association for Computational Linguistics.

Aggarwal, C., & Zhai, C. (2012). *Mining text data*. Springer Science & Business Media.

Baldini, N., Neri, F., & Pettoni, M. (2007). A Multilanguage platform for Open Source Intelligence. *8th International Conference on Data, Text and Web Mining and their Business Applications* (pp. 18-20). The New Forest (UK).

BBC News Europe. (2015, 1 3). *Ukraine crisis: Timeline*. Retrieved from www.bbc.com: http://www.bbc.com/news/world-middle-east-26248275

Berendt, B., & Subasic, I. (2009). STORIES in time: a graph-based interface for news tracking and discovery. *Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology - Volume 03* (pp. 531-534). IEEE Computer Society.

Best, C. (2008). Open Source Intelligence. In F. Fogelman-Soulié, *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security* (pp. 331-343). IOS Press.

Brockwell, P. J., & Davis, R. A. (2002). *Introduction to time series and forecasting*. Taylor & Francis.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys* (CSUR).

Dean, J., & Ghemawat, S. (2008, January). MapReduce: Simplified Data Processing on Large Clusters. *Communications of the ACM*, 51(1), 107-113.

Deng, L., Xu, B., Zhang, L., Han, Y., Zhou, B., & Zou, P. (2013). Tracking the Evolution of Public Concerns in Social Media. *Proceedings of the Fifth International Conference on Internet Multimedia Computing and Service* (pp. 353-357). ACM.

Esling, P., & Agon, C. (2012). Time-series data mining. *ACM Computing Surveys (CSUR)*.

Etzioni, O., Cafarella, M., Downey, D., Popescu, A.-M., Shaked, T., Soderland, S., . . . Yates, A. (2005). Unsupervised named-entity extraction from the web: An experimental study. *Artificial Intelligence, 165*(1), 91-134.

Expert System s.p.a. (2014, 12 13). *Cogito API*. Retrieved from Expert System: http://www.cogitoapi.com/success-stories/intelligence/

Expert System s.p.a. (2015, March 6). *Cogito® Itelligence API live demo*. Retrieved from Cogito® Itelligence API: www.intelligenceapi.com/demo/

Gephi.org. (2014, December 18). *Gephi - The open GraphViz platform*. Retrieved from Gephi: https://gephi.github.io/

Glassman, M., & Kang, M. J. (2012, March). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673-682.

Godbole, N., Srinivasaiah, M., & Skiena, S. (2011). Large-Scale Sentiment Analysis for News and Blogs. *Proceedings of the International Conference on Weblogs and Social Media (ICWSM 2011)*. Boulder, Colorado, USA.

Hamilton, J. D. (1994). *Time series analysis*. Princeton: Princeton University Press.

Holt, C. C. (2004). Forecasting seasonals and trends by exponentially weighted moving averages. *International Journal of Forecasting*, 5-10.

Holzschuher, F., & Peinl, R. (2013). Performance of graph query languages: comparison of cypher, gremlin and native access in neo4j. *Proceedings of the Joint EDBT/ICDT 2013 Workshops*. ACM.

Ihrig, C. J. (2013). JavaScript Object Notation. In C. J. Ihrig, *Pro Node.js for Developers* (pp. 263-270). Apress.

Neri, F., Aliprandi, C., & Camillo, F. (2011). Mining the Web to Monitor the Political Consensus. *Counterterrorism and Open Source Intelligence, Lecture Notes in Social Networks*. Springer-Verlang.

Nguyen, D., Lenharth, A., & Pingali, K. (2013). A lightweight infrastructure for graph analytics. *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*. ACM.

Nisar, M. U., Fard, A., & Miller, J. A. (2013). Techniques for graph analytics on big data. *Proceedings of the 2013 IEEE International Congress on Big Data*, (pp. 255-262).

Odersky, M., Spoon, L., & Venners, B. (2008). *Programming in Scala*. Artima Inc.

Pak, A., & Paroubek, P. (2010). Twitter as a Corpus for Sentiment Analysis and Opinion Mining. *Proceedings of the 7th Language Resources and Evaluation Conference - LREC 2010* (pp. 1320-1326). ELRA.

Pang, B., & Lee, L. (2008). Opinion Mining and Sentiment Analysis. *Foundations and Trends in Information Retrieval*, 1-135.

Paşca, M., Lin, D., Bigham, J., Lifchits, A., & Jain, A. (2006). Names and similarities on the web: fact extraction in the fast lane. *Proceedings of the 21st International Conference on Computational Linguistics and the 44th annual meeting of the Association for Computational Linguistics* (pp. 809-816). Association for Computational Linguistics.

Richard A. Best, A. C. (2008). Open Source Intelligence (OSINT); Issues for Congress. In T. M. Paulson, *Intelligence Issues and Developments* (pp. 75-97). Nova Science Publishers Inc.

Steele, R. D. (2007). Open source intelligence. In L. K. Johnson, *Handbook of Intelligence Studies* (pp. 129-147). Routledge.

Tausch, N., Philippsen, M., & Adersberger, J. (2011). A Statically Typed Query Language for Property Graphs. *Proceedings of the 15th Symposium on International Database Engineering and Applications* (pp. 219-225). Lisboa, Portugal: ACM.

Tosi, S., Casolari, S., & Colajanni, M. (2013). Data clustering based on correlation analysis applied to highly variable domains. *Computer Networks*, 3025-3038.

Wanner, F., Stoffel, A., Jäckle, D., Kwon, B. C., Weiler, A., & Keim, D. A. (2014). State-of-the-Art Report of Visual Analysis for Event Detection in Text Data Stream. *Proceedings of EuroVis - STARs 2014*. The Eurographics Association.

Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., & Stoica, I. (2010). Spark: cluster computing with working sets. *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing* (pp. 10-17). USENIX.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

A Renewed Approach to Serious Games for Cyber Security

Alexis Le Compte
De Montfort University
Leicester, England
alexis.lecompte@dmu.ac.uk

David Elizondo
De Montfort University
Leicester, England
elizondo@dmu.ac.uk

Tim Watson
WMG
University of Warwick
Warwick, England
tw@warwick.ac.uk

Abstract: We are living in a world which is continually evolving and where modern conflicts have moved to the cyber domain. In its 2010 Strategic Concept, NATO affirmed its engagement to reinforce the defence and deterrence of its state members. In this light, it has been suggested that the gamification of training and education for cyber security will be beneficial. Although serious games have demonstrated pedagogic effectiveness in this field, they have only been used in a limited number of contexts, revealing some limitations. Thus, it is argued that serious games could be used in informal contexts while achieving similar pedagogic results. It is also argued that the use of such a serious game could potentially reach a larger audience than existing serious games, while complying with national cyber strategies. To this end, a framework for designing serious games which are aimed at raising an awareness of cyber security to those with little or no knowledge of the subject is presented. The framework, based upon existing frameworks and methodologies, is also accompanied with a set of cyber security skills, itself based upon content extracted from government sponsored awareness campaigns, and a method of integrating these skills into the framework. Finally, future research will be conducted to refine the framework and to improve the set of cyber security related skills in order to suit a larger range of players. A proof of concept will also be designed in order to collect empirical data and to validate the effectiveness of the framework.

Keywords: *serious games, framework, cyber security*

1. INTRODUCTION

The development of technology and the increasing number of cyber threats have led political and military organisations, such as NATO and its state members, to develop cyber security strategies, providing recommendations on how to improve nations' resilience and deterrence.

These strategies focus in particular on the reinforcement of infrastructures and the improvement of businesses practices, but their scope also extends to an individual level, with the objective of training cyber security elites and to educate the general population to fight more efficiently against cybercrime. From a certain perspective, it could be argued that the education of the population represents a cornerstone of the system as citizens constitute both the basis of all actors involved in the development of cyber capabilities (cyber experts, specialised industries, military organisations); and the target of various cyber threats, which needs to be protected and defended (businesses, governments, critical infrastructures, general population). A more educated nation provides better prepared individuals for organisations, but also hinders the spread of cybercrimes.

In parallel, serious games, which commonly refer to games with purposes beyond pure entertainment, have gained a lot of popularity in academia and industry over the past decade due to their pedagogical benefits. As a result, it has been proposed that games are used in information assurance and cyber security for educational and training purposes [1], [2].

However, all of the serious games for cyber security awareness, education and training developed to date have been designed to be used in formal contexts and have aimed at reproducing real life experience.

This paper aims at introducing a different approach to serious games in order to raise awareness of cyber security among the general population. Such a game would consistently fulfil cyber security strategies' objectives in terms of education and awareness. To support this approach, a comprehensive framework for designing and releasing serious games is proposed, based upon a study and a review of existing frameworks and methodologies.

The following section presents a review of serious games, in order to identify the respective strength and limitations of these games. Then, the proposed framework is described in greater detail, and finally, the next section introduces a method of integrating cyber related skills into the framework.

2. SERIOUS GAMES

A. Definition

The expression "serious games" in its modern meaning seems to have been introduced by Abt in 1970 [3] and has since been redefined by many researchers and professionals. A popular definition was given by Zyda who describes serious games as "a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives" [4]. However, the definition of the expression still arouses debate, and Sawyer, who created the Serious Games Initiative in 2002 [5], criticised the variations between existing interpretations, arguing that many authors restrict the definition of serious games based upon their own needs [6].

Although the examples used all relate to video games, the interpretation presented in this paper is not limited to video games and could extend to board games or any other type of games. Furthermore, this paper aims at emphasising the importance of the gaming aspect as a fundamental and non-negligible feature of serious games. Despite the involvement of academics or professional in the conception of serious games for training or educational purposes, serious games should be, primarily, games. This also represents the difference between serious games and gamification, with the latter applying game mechanics to real life contexts. Therefore the expression serious games will simply be defined as "games which incorporate pedagogic elements".

B. Review of Serious Games for Information Assurance and Cyber Security

Serious games have received a fair amount of attention in the field of information security and cyber security, both from academic researchers and in industry.

One of the most popular examples which can be found in the literature is the game "CyberCIEGE", created by the US Naval Postgraduate School (NPS) and sponsored by several US organisations [7], [8]. The game offers a realistic virtual world in which players have to operate and defend a computer network. From a pedagogic point of view, the game encompasses seven fundamental cyber security related topics. The game has also been the object of many academic publications and has shown good pedagogic benefits.

Other examples developed by various US military departments, universities and other organisations, are presented by Pastor *et al*. [9] in a state of the art simulation systems for information security education, training and awareness. Although the paper is focused on simulation systems, the distinction between serious games and pure simulation tools is quite blurred in this context. In particular, the paper mentions CyberCIEGE as part of the list of simulation tools, but describes it as a video game. The paper ultimately proposes a taxonomy of simulation systems, based upon topics, technical features, target audiences, didactical capabilities and so on. Nevertheless, Pastor *et al*. highlighted several limitations in the conclusion of their paper. Firstly, they suggested that more tools should be developed for anyone interested professionally in information assurance, rather than mainly targeting university students. Secondly, they remarked that these tools should allow players to practice in their own environment. Thirdly, they commented that there was very little diversity in the choice of simulations for information assurance teaching, training and awareness.

CyberCIEGE, along with other games like "CyberProtect" or "Anti-Phishing Phil" were cited as examples in a paper from Nagarajan *et al*. [10]. In this paper, the authors conducted research on game design for cyber security training emphasising particularly on a game called

“CyberNEXS”. The latter contains different modes, respectively focusing on computer network, forensics and penetration testing. While the authors aimed at producing a game addressing limitations of existing training solutions, they use CyberNEXS as a basis for improvements. To this end, they elaborate on game genres and game mechanics, providing examples directly applicable to CyberNEXS.

Anti-Phishing Phil was developed at Carnegie Melon University to provide a user friendly tool to teach about phishing attacks. In this game, players have to guide a fish towards different worms that will display a genuine or a phishing link. Players then have to identify whether the link is legitimate or not by choosing to “eat” or “reject” the worm. In a paper dedicated to the game, Sheng *et al*. [11] present the methodology and the structure of the game, concluding on the results of their user study showing the best outcomes when playing the game.

Several other games can be found in industry. “Data Security”, “Agent Surefire”, “Cyber Awareness Challenge” and “Cyber Security Investigation (CSI) Game” are four games covering information assurance and cyber security topics. In the simulation game “Data Security”, from Playgen [12], players play the role of a new employee tasked to identify security concerns. “Agent Surefire”, produced by Mavi Interactive [13], [14] , is a point and click simulation in which players must catch an insider threat, identify breaches and security issues. According to Mavi Interactive, the game has been really well received in industry, receiving a total of thirty-six awards. “Cyber Awareness Challenge”, developed by Carney, Inc. [15] is also a simulation. This game, which was one of the finalists of the “2012 Serious Games Showcase & Challenge”, proposes mini games as a federal government agent whose purpose is to capture an unnamed hacker. The last example, “Cyber Security Investigation (CSI) Game”, developed by InfoSecure [16], and which will be fully finished later this year, is a kind of puzzle game, where players have to find the right combination of events that led to an information security incident.

It is also worth citing the game “Secure Futures”, released on the website “Big Ambition” [17] developed by e-skills UK, the Sector Skills Council for Business and Information Technology in UK. The game, which targets pupils, introduces cyber security careers and is accompanied with teaching guides for teachers. After registering, the game is freely available to play. After trying the game, it was found that the scenario was interesting from a technical point of view and that the website was easy to navigate. However, it could be argued that this game may be too difficult for young players which led to uncertainties about its pedagogic effectiveness. Nevertheless, without proper analysis, it is impossible to make any conclusions on this point; furthermore, the game was not designed to teach cyber security, but rather to provide an overview of careers in this field.

Finally, when looking at games from the traditional gaming industry, no example of serious games on cyber security was found. A few games on the theme of “hackers” exist, such as “Uplink” [18] or “Hacker Evolution” [19], which let players fulfil various missions as professional hackers in a virtual world, but these games are not designed to teach any specific concepts and therefore cannot be considered as serious games.

C. Observations and Suggestions

When reviewing the aforementioned academic publications and commercial products, it appears clearly that serious games present a great pedagogic potential for cyber security awareness, teaching and training, as evidenced by case studies. The large number of industry awards received by some of these games also shows that businesses approve their usefulness and effectiveness.

Nevertheless, several limitations arise from the presentation of these games:

1. In their attempt to immerse players in a realistic environment, most of these games are simulation based games, or are strongly aiming at reproducing real life scenarios. This observation is also corroborated by Connolly et al. [20] who conducted a literature review of empirical evidence on serious games which shows that simulation was the most popular game genre in their research results. However, the excess of simulation based games could lead to the potentially wrong assumption that it is the only viable game genre for serious games design. On the contrary, Nagarajan *et al*. [10] show that many different game genres could embody cyber security related concepts, based upon different game mechanics. Furthermore, different game genres would suit a wider range of players, as different players have different game preferences.
2. In most cases, the examples shown previously are designed for educational purposes for use in school or in university, or for training purposes in corporate environment. This implies that the access to most of these games is tied to a formal environment (school, university, business, etc. Marklund *et al*. [21] explained in great details the difference between formal and informal contexts), sometimes under the supervision of a learning facilitator or an instructor, and that players rarely have the possibility to play these games outside of these contexts, by their own initiative. This leads to several issues already highlighted by Nagarajan *et al*. [10], such as the lack of continual practice necessary to a better knowledge retention or too much information in too little time, among several other issues. Thus, Pastor et al. [9] argued that players should be able to play the game "in their own environment" in order to get a deeper understanding of concepts presented in games; which was confirmed by Thompson and Irvine [22] who shown in a study on CyberCIEGE that the ability to play the game on personal computers substantially improved the educational experience.
3. In a slightly similar perspective, it can observed that none of these games can be acquired through traditional distribution channels for video games such as online store or video games shops, nor are they mentioned on entertainment video games forums. Instead, these games are sometimes available from their respective official website, or on request from the organisations producing them. It appears that there exists a gap between serious games and entertainment games, and that as a result, it could be argued that serious games fail to reach large audiences and that their potential is only exploited in formal contexts. Indeed, only people aware and convinced of the benefits of serious games will promote and implement serious games in their organisation or business. To come back to the context of NATO and cyber security policies, the education and the development of competences through serious games

would mostly rely on the responsibility of a somewhat limited number of schools, universities and business.

4. From a technical perspective, a direct consequence of serious games being essentially designed for formal contexts is the added complexity in the development process and implementation. This problem is in particular illustrated by Marklund *et al*. [21] who proposed a model for balancing pedagogic and players expectations. By designing serious games for "informal" contexts, many constraints and issues listed by Nagarajan *et al*. [10] and Marklund *et al*. [21] can be removed, in particular the need for a well structured environment and supervisors. Players would just acquire the game and built their own environment in order to play the game. Also, there is a limit to how many hours serious games can be used in formal contexts, whereas this restriction virtually does not exist in informal contexts.

Based upon all these observations, it can be argued that it is technically possible to design serious games for use in informal contexts which could be pedagogically viable.

To support this theory, the game "Wii Fit", and its sequel "Wii Fit plus", from the Japanese firm Nintendo, can be used as examples. The games propose various types of fitness exercises and rely on the use of a special board. While these games achieved noticeable commercial results, with 22 millions of copies sold for "Wii Fit" and around 20 million for its sequel [23], [24], the games have also demonstrated pedagogic usefulness and effectiveness. "Wii Fit" was used in several health studies and shown positive results [25–27].

To put it in a nutshell, millions of people have played Wii Fit, in informal contexts, over variable periods of time, most likely from their own initiative and may have purchased its sequel. Although these games were primarily designed as flagships for Nintendo's console, their popularity combined to empirical evidences acquired through academic studies would suggest that the games have had a positive pedagogic impact on players. It is also unclear if these games have had an impact in the long term, but the same observation can be made for serious games used in formal contexts. Nevertheless, it appears that two different paradigms are possible, and that pedagogic outcomes can be achieved in both cases. What is more, developing serious games for cyber security teaching, training and awareness for informal contexts would open new perspectives in terms of self-education. Serious games designed for informal contexts have the potential to reach and spread across a larger and more diversified audience. It can even be imagined that well designed serious games could keep users playing over longer periods of time, increasing the frequency of practicing pedagogic concepts through the games.

3. PROPOSED FRAMEWORK

Due to the growing popularity of serious games, much research has been conducted on design methodologies for serious games, as illustrated by the publication of MSc or PhD thesis and other academic papers [28–30]. Despite this, some researchers have focused on specific aspect of serious games design, highlighting limitations and issues or suggesting new approaches, in particular in the design and evaluation of serious games.

As a basis for a comprehensive framework to design serious games aimed at informal contexts, essential steps were extracted from existing frameworks and methodologies, resulting in a generic and iterative set of steps which can be applied to most serious games. The limitations raised in the literature were also taken into account, and each step is supported by one or several concepts developed specifically to address these limitations. Finally, particular emphasis was laid on the development and deployment processes in order to make the framework more suitable for informal contexts.

Step 1: Preliminary analysis.

Poor project management and planning are responsible for more than half of IT project failure, and video games are no exceptions. This crucial step essentially consists in defining the pedagogic objectives for the game, gathering information about the target audience and analysing the technical constraints for the development of the game. The objectives of these steps are:

- Evaluating the technical resources allocated for the development of the game. This includes equipment but also time constraints, budget and technical skills of the developers. All these factors have an impact on the quality of the final game and must therefore be analysed carefully in order to maximise the success rate of the overall development process and distribution
- Defining pedagogic objectives. A set of key skills must be clearly identified. These skills will be matched against game mechanics later on
- Identifying target players and context of play (as described by the Design, Play, Experience framework (DPE) [31] and the Four Dimensional Framework (FDF) [32]). Players will have different expectations from the game depending on their cultural background or experience. Thus, understanding the players help in providing a more suitable game, adapted to the targeted players
- Defining the pedagogic and game mechanics (as described by the LM-GM framework). Pedagogic objectives can be associated to game mechanics to produce consistent gameplay. Choosing appropriate game mechanics is also essential in order to choose a game genre. A customised LM-GM map is proposed in the next section.

Step 2: Design.

The design is all about building conceptual models. The key characteristics for these models should present a balance between serious objectives and entertainment:

- From a technical point of view, models can be formalised with the help of the LM-GM [33] and the DPE framework [31]. They will ensure consistency between pedagogic mechanics and game mechanics, while concentrating on the players perspective in order to provide engaging gameplay for players
- Developers should ensure that the purposes of the game are well conveyed through the game, as explained by the SGDA framework [34]. Clear objectives not only generate a greater engagement of players, but also help them to better assimilate the pedagogic objectives
- Games should present a progressive level of difficulty, with in-game tutorials and many opportunities to practice. Gee [35] also suggests that games should provide opportunities where skills acquired in game will not be sufficient to progress,

requiring players to develop new techniques by themselves. This contributes to a more engaging gameplay but also stimulates players' creativity. It is essential that models developed at this stage incorporate the techniques used by entertainment games as they will help to build better quality games, and more engaging games. A direct consequence of this is that players will give more attention to pedagogic objectives

Step 3: Development.

The purpose of this stage is to provide technical guidance to develop the game while respecting the constraints identified during step 1. In particular this steps guides developers in the choice for a suitable approach to the development of games. The aim is to provide the best balance between time, skills and financial limitations:

- Support from a third party: Some companies, with the example of Mavi Interactive, specialise in the development of serious games, and can provide either ready to use games, or provide support for the development of customised games. This solution will come at a cost, and can be time consuming.
- Off-the-shelf game: An existing game, from an entertainment game studio or a specialised development company, can be used in a teaching or training context. In this case, learning facilitators may be involved in the deployment and use of the game, and may provide additional guidance and instructions for pedagogic objectives to fulfil, which means that players may not be able to play the game without supervision. However, from a technical point of view, this solution is efficient as it considerably simplifies the development process and removes the need for developers.
- Off-the-shelf game with modifications: Some existing games enable players and developers to customise the original game by adding additional content in game referred to as "mods", which can be used to introduce the pedagogic objectives while maintaining the integrity of the original game. This solution can be useful as players may not necessarily need to be monitored or guided by learning facilitators, and can be autonomous when playing the game. On a technical side, this solution can also be time and cost effective, as it may only require a limited amount of development.
- Assisted development: To mitigate the difficulties of video game development and improve the production ratio, assisted methodologies have been developed. These methodologies are usually accompanied with tool kits which simplify the development process. For instance, the EMERGO methodology [36] proposes a 5 step methodology, from the analysis to the evaluation, with tools assisting with the completion of each of these steps and requiring a minimum amount of programming. The end result is an interactive video based game, which can be played in web browsers. The downside with such a choice is that the options for customisations are limited and complex scenarios may be difficult to implement.
- Full development: If the development team has the appropriate knowledge, the time and financial resources, it is also possible to build a game from scratch. In this case, the development team is completely responsible for all phases of the development. The time and financial cost of the game will depend on the competence of the development team and the game to be built.

Step 4: Game assessment.

Game assessment is a crucial part of the development process and could be compared to user acceptance in software development. This step has the objective of ensuring that the game matches technical and pedagogic expectations, while maximising players' engagement and enjoyment.

- Several frameworks have been designed to evaluate serious games and players ([37], [38]). One of the most recent studies was conducted by Mayer [39], who highlighted limitations of existing frameworks and developed a comprehensive methodology, which is generic enough to be applied in numerous contexts (education, training, professional environment...).
- In the video game industry, engagement and enjoyment are usually estimated through testing phases. Players can either be recruited or they can obtain copies of prototypes to test the game before its release. Feedback from players are then collected, either via survey or directly in game, so that developers can uncover bugs, improve gameplay or even modify game mechanics if the game does not match their initial expectations. These testing phases are also important for the reputation of the game as they constitute its first public exposure, and are often accompanied with trailers or reviews of the prototype.

Step 5: Deployment.

In formal contexts, rules apply to the deployment of serious games. Most often, players are supervised by an instructor or a learning facilitator, time is limited and play sessions are framed within the pedagogic plan. In informal contexts, the constraints and requirements are different. Nevertheless, the release process is an integral part of the lifecycle of a commercial product, and the gaming industry already uses techniques to maximise sales and reach large audiences. This implies the use of marketing campaigns, supported by advertisements, demonstrations, the creation of dedicated websites and a presence on social media. These techniques should also be applied to serious games, and could in fact increase the benefits of the games. For instance, Gee [35] provided empirical evidences of the benefits of using external media such as forums, and Raybourn [40] even demonstrated that transmedia strategies is key for new learning strategies.

Step 6: Player assessment.

Finally, to determine whether games contribute to skills improvement, it is necessary to evaluate players. This can be done following Mayer's methodology [39], or game mechanics can be implemented in order to evaluate players directly while playing. Indeed, most games become increasingly difficult as players progress throughout the game. Thus, to progress, players need to master particular skills and principles [35]. If pedagogic mechanics are appropriately mapped to game mechanics, then players should acquire the expected skills when completing the game.

Tests, surveys and questionnaires could potentially be used, but would have to be implemented in a way which does not require an external intervention since the aim is to deploy serious games in informal contexts.

4. INTEGRATING CYBER SKILLS IN SERIOUS GAMES

Cyber security is a field with multiple, technically complex and ever changing aspects, and cyber threats can affect individuals as well as large organisations like businesses or governments. As a consequence, there is a real need to educate people to the most basic cyber security principles.

In the UK, for instance, the government deployed its cyber security strategy in order to provide guidance to businesses and to inform the public. This resulted in the creation of public awareness campaigns and websites such as “Get safe online” [41] or “Cyber Streetwise” [42] which cover an exhaustive list of topics such as protecting computers or users, online behaviour or safeguarding children but also guidance on physical security, backups, staff management, legal advice and so on. Although the content provided on these websites is not in as great depth as other sources such as the IISP skills framework [43] or the Skills Framework for the Information Age [44], which both emphasise on information security in businesses, the two campaigns have the advantage of being simple enough while covering the most common cyber threats. Therefore, the knowledge presented in these two websites are relevant for people with no prior or limited knowledge in cyber security, but can also be relevant to those who have already understood these basics, as a reminder. However, as Gee suggests [35], well designed video games encompass good educational practices. Thus, serious games for cyber security awareness should implement gradually complex concepts, starting with the most basic aspects of cyber security. One of the objectives of this paper is to focus on basic concepts and awareness of the general public, therefore, concepts specifically applying to businesses or requiring prior knowledge in cyber security will be avoided. More advanced sets of topics would be more suitable in the context of advanced training, for people with experience or knowledge of cyber security or for specific businesses. These topics may be integrated in a future update of this framework.

In order to fit an appropriate set of skills into the framework, relevant competences were first extracted from “Get Safe Online” and “Cyber Streetwise”. This compilation of skills was then used to enhance the model presented in the “Learning Mechanics - Game Mechanics” (LM-GM) framework [33] (see Table I). To use the resulting customised LM-GM map, the learning mechanics grid should be used as a transitional layer between cyber security skills and game mechanics.

TABLE 1: CUSTOMISED LM-GM MAP WITH CYBER SECURITY SKILLS

	CYBER SECURITY SKILLS	
Use of appropriate hardware	Proper hardware disposal	
	Backing up data on separate devices	
Software updates	Using appropriate encryption	Using security software (anti-virus)
	Avoiding remote access / online services	
Using strong passwords	Avoiding disclosing personal information	Avoiding untrusted / unknown networks
	Secure online payment / mobile banking	
Being able to identify potentially dangerous searches	Being able to identify social engineering	Being able to identify and react to cyber threats and cyber frauds *
Controlling and monitoring people with physical / remote access to assets	Protecting access to critical assets (machines and networks)	Establishing usage rules
	Being able to identify legal from illegal use of a computer or software	

* scams, phising, cyberbullying, cyberstalking, money mulling, blackmail, ransomware...

	LEARNING MECHANICS	
Instructional	Guidance	
Demonstration	Participation	Action / Task
Generalisation / Discrimination	Observation	Feedback
	Question & Answer	
Explore	Identify	Discover
	Plan	Objectify
Hypothesis	Exeperimentation	
	Repetition	
	Reflect / Discuss	Analyse
	Imitation	Shadowing
Simulation	Modelling	
Tutorial	Assessment	
	Competition	
Motivation	Ownership	Accountability
	Responsibility	Incentive

	GAME MECHANICS		
Behavioural Momentum	Role Play		
Cooperation	Collaboration	Goods / Information	
Selecting / Collecting	Tokens	Cut Scenes /Story	
	Cascading Information	Communal Discovery	
	Questions & Answers	Pareto Optimal	Appointment
Strategy / Planning	Resource Management	Infinite Gameplay	
Capture / Eliminate	Tiles / Grids	Levels	
Game Turns	Action Points	Feedback	
Time pressure	Pavlovian Interactions	Meta-game	
	Protégé effects	Simulate / Response	Realism
Design / Editing	Movement		
Tutorial	Assessment		
	Competition		
Urgent Optimism	Ownership		
Rewards / Penalties	Status	Virality	

5. CONCLUSIONS AND FUTURE WORK

This paper reviewed existing serious games for cyber security awareness, teaching and training, showing that these games have a great pedagogic potential. However, their use is most often limited to formal contexts, leading to several limitations. It was argued that these limitations could be overcome if serious games were released in informal contexts, without degrading their pedagogic virtues.

In this perspective, a framework balancing pedagogic and game mechanics has been proposed, which also suggests an approach supported by transmedia theories [40], more in line with entertainment games, for the deployment of serious games. Finally, a method of integrating cyber security related skills, based upon the LM-GM framework, has been presented.

Future work will focus on improving the set of cyber related skills, in order to provide an appropriate set of skills for different level of expertise, and therefore cover a larger range of players. Research will also be conducted on alternative methods for integrating pedagogic content in games. Finally, a proof of concept will be designed for a case study in order to refine and validate the framework.

REFERENCES

[1] J. A. Amorim, M. Hendrix, S. F. Andler, and P. M. Gustavsson, “Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment,” in *NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111)*, 2013.

[2] “Serious Games and their Use in NATO,” in *NATO Modelling and Simulation Group (MSG) Lecture series (STO-EN-MSG-115)*, 2013.

[3] D. Djaouti, J. Alvarez, J.-P. Jessel, and O. Rampnoux, “Origins of Serious Games,” in *Serious Games and Edutainment Applications*, M. Ma, A. Oikonomou, and L. C. Jain, Eds. Springer London, 2011, pp. 25–43.

[4] M. Zyda, “From visual simulation to virtual reality to games,” *Computer*, vol. 38, no. 9, pp. 25–32, 2005.

[5] The Serious Games Initiative, “Serious Games Initiative.” [Online] http://www.seriousgames.org/ [Accessed 20/02/14].

[6] B. Sawyer and P. Smith, “Serious Games Taxonomy.”, [Online] http://www.dmill.com/presentations/serious-games-taxonomy-2008.pdf? [Accessed 8/03/14], 2008.

[7] Centre for Information Systems Security Studies and Research (CISR), “Incorporating CyberCIEGE into an Introductory Cyber Security Course.”, [Online] http://cisr.nps.edu/cyberciege/CyberCIEGE%20Syllabus.html [Accessed 5/12/2014], 2013.

[8] Centre for Information Systems Security Studies and Research (CISR), “Incorporating CyberCIEGE into an Introductory Cyber Security Course.”, [Online] http://cisr.nps.edu/cyberciege/CyberCIEGE%20Syllabus.html [Accessed 5/12/2014], 2013.

[9] V. Pastor, G. Díaz, and M. Castro, “State-of-the-art simulation systems for information security education, training and awareness,” in *Education Engineering (EDUCON), 2010 IEEE*, 2010, pp. 1907–1916.

[10] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, “Exploring game design for cybersecurity training,” in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*, 2012, pp. 256–262.

[11] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish,” *Institute for Software Research*, 2007.

[12] Playgen, “Data Security.”, [Online] http://playgen.com/play/data-security/ [Accessed 5/12/2014].

[13] Mavi Interactive, “Agent Surefire.”, [Online] http://www.maviinteractive.com/agent_surefire_insider_threat.asp [Accessed 5/12/2014].

[14] E. Alhadeff, “Converting Cybersecurity Practice Into Engaging Serious Games.”, [Online] http://seriousgamesmarket.blogspot.co.uk/2012/02/converting-cybersecurity-practice-into.html [Accessed 09/03/2015], 2012.

[15] E. Alhadeff, “Serious Games As Information Assurance Adventures.”, [Online] http://seriousgamesmarket.blogspot.co.uk/2012/12/serious-games-as-information-assurance.html [Accessed 09/03/2015], 2012.

[16] InfoSecure, “Cyber Security Investigation Game.”, [Online] http://www.infosecuregroup.com/CSI.html [Accessed 10/03/2015], 2015.

[17] Big Ambition, “Secure Futures.”, [Online] http://www.bigambition.co.uk/securefutures [Accessed 5/12/2014].

[18] Introversion Software, “Uplink.”, [Online] http://www.introversion.co.uk/uplink/index.html [Accessed 8/12/2014].

[19] Exosyphn Studios, “Hacker Evolution.”, [Online] http://www.exosyphen.com/page_hackerevolution.html [Accessed 9/12/14].

[20] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle, “A systematic literature review of empirical evidence on computer games and serious games,” *Computers & Education*, vol. 59, no. 2, pp. 661–686, 2012.

[21] B. B. Marklund, P. Backlund, and H. Engstrom, “The Practicalities of Educational Games: Challenges of Taking Games into Formal Educational Settings,” in *Games and Virtual Worlds for Serious Applications (VS-GAMES), 2014 6th International Conference on*, 2014, pp. 1–8.

[22] M. Thompson and C. Irvine, “Active Learning with the CyberCIEGE Video Game,” in *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, 2011, pp. 10–10.

[23] Nintendo, “It’s official! Nintendo’s Wii Balance Board is a record breaker!”, [Online] https://www.nintendo.co.uk/News/2012/It-s-official-Nintendo-s-Wii-Balance-Board-is-a-record-breaker--253133.html [Accessed 10/12/14], 2012.

[24] Nintendo Co., Ltd., “Financial Results Briefing for Fiscal Year Ended March 2012.”, [Online] http://www.nintendo.co.jp/ir/pdf/2012/120427e.pdf [Accessed 10/12/14], 2012.

[25] N. B. Herz, S. H. Mehta, K. D. Sethi, P. Jackson, P. Hall, and J. C. Morgan, “Nintendo Wii rehabilitation (‘Wii-hab’) provides benefits in Parkinson’s disease,” *Parkinsonism & Related Disorders*, vol. 19, no. 11, pp. 1039–1042, 2013.

[26] R. Mombarg, D. Jelsma, and E. Hartman, “Effect of Wii-intervention on balance of children with poor motor performance,” *Research in Developmental Disabilities*, vol. 34, no. 9, pp. 2996–3003, 2013.

[27] N. Vernadakis, A. Gioftsidou, P. Antoniou, D. Ioannidis, and M. Giannousi, “The impact of Nintendo Wii to physical education students’ balance compared to the traditional approaches,” *Computers & Education*, vol. 59, no. 2, pp. 196–205, 2012.

[28] C. Bull-Hansen, “Serious Games: Video Game Design Techniques for Academic and Commercial Communication.,” University of Oslo, 2007.

[29] D. Fitchie, “Investigating the use of Serious Games for teaching anatomy and physiology to higher education students: Research into Serious Games,” University of Huddersfield, 2011.

[30] A. Yusoff, “A Conceptual Framework for Serious Games and its Validation,” University of Southampton, 2010.

[31] B. Winn, “The design, play, and experience framework,” *Handbook of research on effective electronic gaming in education*, vol. 3, pp. 1010–1024, 2008.

[32] S. de Freitas and M. Oliver, “How can exploratory learning with games and simulations within the curriculum be most effectively evaluated?,” *Computers & Education*, vol. 46, no. 3, pp. 249–264, 2006.

[33] S. Arnab, T. Lim, M. B. Carvalho, F. Bellotti, S. de Freitas, S. Louchart, N. Suttie, R. Berta, and A. De Gloria, “Mapping learning and game mechanics for serious games analysis,” *British Journal of Educational Technology*, 2014.

[34] K. Mitgutsch and N. Alvarado, “Purposeful by Design?: A Serious Game Design Assessment Framework,” in *Proceedings of the International Conference on the Foundations of Digital Games*, 2012, pp. 121–128.

[35] J. P. Gee, *What video games have to teach us about learning and literacy*. Palgrave Macmillan, 2007.

[36] R. J. Nadolski, H. G. K. Hummel, H. J. van den Brink, R. E. Hoefakker, A. Slootmaker, H. J. Kurvers, and J. Storm, “EMERGO: A methodology and toolkit for developing serious games in higher education,” *Simulation and Gaming*, vol. 39, no. 3, pp. 338–352, 2008.

[37] T. Connolly, M. Stansfield, and T. Hainey, “Towards the Development of a Games-based Learning Evaluation Framework,” in *Games-based Learning Advancement for Multisensory Human Computer Interfaces: Techniques and Effective Practices*, Idea-Group Publishing: Hershey, 2009.

[38] A. Yusoff, R. Crowder, and L. Gilbert, “Validation of Serious Games Attributes Using the Technology Acceptance Model,” in *Games and Virtual Worlds for Serious Applications (VS-GAMES), 2010 Second International Conference on*, 2010, pp. 45–51.

[39] I. Mayer, “Towards a Comprehensive Methodology for the Research and Evaluation of Serious Games,” *Procedia Computer Science*, vol. 15, no. 0, pp. 233–247, 2012.

[40] E. M. Raybourn, “A new paradigm for serious games: Transmedia learning for more effective training and education,” *Journal of Computational Science*, vol. 5, no. 3, pp. 471–481, 2014.

[41] Get Safe Online, “Free online security advice.”, [Online] https://www.getsafeonline.org/ [accessed 20/12/2014].

[42] HM. Government, “Cyber Street, Protect your home or business from cyber crime.”, [Online] https://www.cyberstreetwise.com/ [accessed 20/12/2014] .

[43] Institute of Information Security Professionals, “Our Skills Framework.”, [Online] https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework.aspx [Accessed 17/11/2014], 2013.

[44] SFIA Foundation, “Skills Framework for the Information Age.”, [Online] http://www.sfia-online.org/ [Accessed 17/11/2014] .

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Exfiltrations Using Polymorphic Blending Techniques: Analysis and Countermeasures

Matteo Casenove
Vrije Universiteit
Amsterdam, The Netherlands
m.casenove@gmail.com

Abstract: Cyber espionage campaigns and cyber attacks make use of data exfiltration on a regular basis causing damages for billions of dollars. Nowadays, they represent one of the primary threats, and they are performed by criminals, companies and states. Normally, data exfiltration uses classic application-layer protocols (e.g. *FTP* or *HTTP*) in combination with very basic obfuscation mechanisms. Even though in most cases these techniques are effective enough, this paper describes how instead they can be detected using properly configured *IDSs*. Moreover, we introduce a novel approach named *polymorphic blending exfiltration* that serves to avoid detection from signature-based as well as anomaly-based *IDSs*. This technique permits to blend the exfiltrated data in the normal and legitimate traffic. We show how *IDSs* can be easily improved in order to be able to detect such exfiltration. Finally, we conclude presenting different evasion techniques that can be included in the polymorphic blending exfiltration to keep providing a safe undetectable exfiltration.

Keywords: *cyber-espionage, exfiltration, obfuscation, IDS*

1. INTRODUCTION

Over the last ten years cyber security has been dealing with the major threat of data loss due to cyber espionage campaigns and cyber attacks. Besides the trivial technical security implications, it also has a substantial economic impact on companies and states; therefore, nowadays, it sits on top of the list of the most dangerous cyber threats. The action commonly associated with stealing data is called *data exfiltration* [1] and it corresponds with moving data without authorisation from a compromised machine to an external drop-zone controlled by the attacker. Security experts strive to secure the internal network from the external one, often overlooking the threats coming from the internal and more trusted network. Within an organization, or a company, information is a critical resource as it carries personal client data, classified company data or any other information that could cause substantial damages to its owner if not adequately protected. Due to its criticality it is called *sensitive information* and it represents the target of the exfiltration activity.

During the exfiltration process, it is crucial that the activity does not raise any suspicion and, most importantly, it is not itself detected. In fact, as soon as the exfiltration is detected, security personnel can stop the attacker's operation and enhance the security level so that the possibility of security breaches decrease. In a computer system, the last actor of the security chain is the *Intrusion Detection System (IDS)* [2], which performs traffic inspection in order to detect malicious activity and - in case - raises an alert. Obviously, in a computer system there can be many other security solutions but in this work we only focus our study on IDSs. Knowing the presence of these security systems, the attacker makes use of different techniques for the purpose of avoiding detection during an exfiltration, such as social engineering, steganography and encryption, or common protocols [3][4]. Many of the detected malware and espionage campaigns have been found to be using a single or a combination of these exfiltration methods [5][6].

In this work we argue that these techniques can be detected not by the conventional *signature-based IDSs* but instead, by the more *advanced anomaly-based IDSs*. Moreover, we propose and implement a more advanced exfiltration technique named *Polymorphic Blending Exfiltration (PBE)* based on the classic *Polymorphic Blending Techniques (PBT)* [7] in order to evade the *anomaly-based IDSs* as well. This technique tries to emulate the normal behaviour of the network to blend the exfiltration in the normal traffic.

The contribution of this work is threefold: a) it shows that *IDSs* can be evaded by using our new polymorphic blending technique, b) it presents a tool that uses this technique successfully against state of the art *IDSs*, and c) it shows that the exfiltration tool can take advantages of the *traffic feature tolerance* allowed by the *IDS* in order to avoid high false-positive rate.

The remainder of the paper is organised as follows. In Section 2 we hand over the very limited literature about exfiltration. Section 3 describes the exfiltration problem and the polymorphic blending technique. In Section 4, the paper presents the exfiltration tool and the tests performed to evaluate its exfiltration performances. Section 5 discusses countermeasures that *IDSs* can apply in order to detect our exfiltration and then what we can improve in our exfiltration technique. Finally, Section 6 contains the conclusions of our work and Section 7 paves the way for future research.

2. RELATED WORKS

The Polymorphic Blending Technique was first addressed by Fogla in [7] and applied only for avoiding detection when sending exploits. The first phase of this technique collects the traffic features and it creates the traffic profile, while it is in the second phase that the real attack happens and the traffic manipulation comes to be. Perdisci *et al*. in [8] presents McPAD, an anomaly-based intrusion detection system able to detect the polymorphic blending attack introduced by Fogla. In our work, we use the polymorphic blending technique by inverting the direction of the attack: instead of sending the attack from the hacker's machine to the target machine, we apply the *PBT* for exfiltrating data from the infected machine to the hacker's device. One of our goals in this work is to test our exfiltration against *McPAD* in order to determine whether it is still able to detect our implementation of the technique.

Amit in [9] and Antwerp in [1] present the most common exfiltration techniques that have been seen in the wild, such as *HTTP Post, FTP, DNS tunnelling, VoIP etc*. The two works describe these methods and how they can be detected. Antwerp in particular provides a framework where to use these methods and where to test the network security.

Wendzel *et al*. in [10] present the concept of Network Steganography. It is the same technique that we call blending: hiding information in the network traffic. They compiled a state-of-the-art survey on several techniques, which use well-known protocols in order to hide information in the network traffic. They use common high-level protocols like *VoIP, P2P*, and *Google* search queries as well as low-level steganography such using *WLANs* padding frames or cross-virtual machine information leakage for Cloud Computing. Moreover, Wandzel in his PhD Thesis [11] provides a very complete and detailed picture on the field of Covert Channels. He describes different techniques and uses of covert channels as well as few solutions able to detect or stop the leakage of information that exploits these channels. Our technique can be seen as a covert channel but, differently to the ones proposed by Wandzel, we do not exploit the protocols injecting extra data in the existing communication, instead we create a new exfiltration connection emulating the content of the packets of the legitimate connections.

Yarochkin *et al*. in [12] introduced a so-called *Network Environment Learning* phase used by covert channel in order to detect the legitimate protocol to use. This learning phase permits to identify the peers of the communication and which are the protocols that can be used as covert channels. In our work, the same technique is used in our collecting phase in order to create the profile for the legitimate traffic.

Khattak *et al*. in [13] discuss the problem of passing through censorship-resistant systems. They present the exfiltration techniques that can be applied to avoid the censorship monitors - in particular the *Great Firewall of China* - by using known *NIDSs* vulnerabilities. They exploit flaws in the *TCP* and vulnerabilities in the *IDSs*.

Houmansadr *et al*. in [14] study the vulnerabilities of censorship-resistant communication systems. These systems just partially implement well-known communication protocols like *Skype* trying to look like legitimate traffic. The research shows the lengthy list of requirements these censorship-resistant communication systems must respect in order to avoid detection and, due to this conspicuous list, the work concludes by stating the failure of the *"unobservability by imitation"* approach.

Fawcett in [15] proposes a possible solution to fill the gap between the advanced exfiltration techniques and the ability of detecting them. He uses the entropy characteristics of network traffic and the observation of the traffic state of encryption in order to distinguish data leakage from benign data. He contributes to the implementation of the detection tool called *ExFILD*, which is able to detect exfiltration from normal traffic by using heuristics on the traffic entropy. In our case, this approach is not effective since with polymorphic blending we tend to maintain the same entropy as the normal traffic.

Bolzoni *et al*. in [16] present *ATLANTIDES*: an architecture for automatic alert verification in network intrusion-detection systems. Using *ATLANTIDES* they intend to reduce the number of false positive by using correlations between the input and output traffic. Unfortunately, the system requires a training phase where it records the normal output traffic per host. In our case, the server represents the host and it is contacted for the first time for the exfiltration and consequently *ATLANTIDES* cannot create any profile.

3. EXFILTRATION

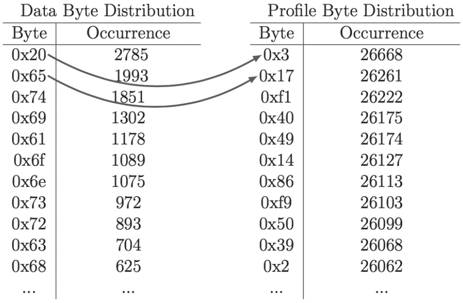
Nowadays, we observe an enormous activity of information theft such as espionage campaigns, credential thefts or intellectual property thefts, and each of them shares a common denominator: the action of extracting sensitive data from an infected machine. This action is called data exfiltration and it targets *sensitive information*, which is defined as information to which an unauthorised loss, misuse, access, modification, or disclosure may produce an adversely security effect [17].

The one and only concern of an exfiltration is to avoid detection of all the security systems placed in the computer system. Among all of them, we only focus on a subset of them such as the so-called Intrusion Detection Systems (*IDSs*). These are monitoring systems designed to detect malicious activities and, upon detection, raise alerts. In order to evade *IDSs*, the attacker uses different methods for exfiltrating data [1]. She can use standard high-level protocols such as *HTTP Post* [18], *DNS Tunnelling* [19], *FTP, Skype* [20], *etc*. trying to make the exfiltration look like a legitimate traffic and avoid suspicions, or she can use transport layer protocols (*TCP* or *UDP*) applying encryption or obfuscation in order to make the *IDSs* deep-packet inspection useless. In the first case, by using standard protocols, the attacker blends the data in the normal traffic, while in the second case she manipulates the data so that it can be unrecognisable. In this work, we use the Polymorphic Blending Technique (*PBT*), which combines the two previously described cases.

A. The Polymorphic Blending Technique

The *PBT* was used for the first time by Fogla in [7] to avoid exploits detection during an attack. The main goal of *PBT* is to perform obfuscation and blend the data in the normal traffic. The polymorphic part of the technique is put in when the obfuscation is applied and it is used for avoiding the detection of *signature-based IDSs (SIDS)*. The blending part instead is used to evade the more advanced *anomaly-based IDSs (AIDS)*. In order to complete these two parts, *PBT* is divided in two phases: the collecting and the blending phases. The preliminary phase of collecting is used to create the traffic profile of the normal traffic. The normal network activities of the infected machine are recorded and analysed with the purpose of creating a traffic profile to emulate. During this phase, only the most significant network features are recorded and those are exactly the same ones used by the *IDSs* to create their profiles. Afterwards, this profile is used in the blending phase to alter the traffic and to make it as similar as possible to legitimate traffic. The blending manipulates the traffic features as well as the payload of the packets by using byte substitution. The profile contains the bytes distribution of the traffic that is the number of occurrences of each byte within the same connection. After that, *PBT* substitutes the bytes of the target data according to the bytes distribution of the profile as shown in Figure 1. In this way, when this data is sent, the payload statistics remain almost the same as the one recorded in the profile.

FIGURE 1: BYTE SUBSTITUITION



Data Byte Distribution		Profile Byte Distribution	
Byte	Occurrence	Byte	Occurrence
0x20	2785	0x3	26668
0x65	1993	0x17	26261
0x74	1851	0xf1	26222
0x69	1302	0x40	26175
0x61	1178	0x49	26174
0x6f	1089	0x14	26127
0x6e	1075	0x86	26113
0x73	972	0xf9	26103
0x72	893	0x50	26099
0x63	704	0x39	26068
0x68	625	0x2	26062
...	...	...	...

Byte substitution is a really easy way to obfuscate data and it is also polymorphic since it changes every time according to the collected traffic.

4. UNDETECTABLE EXFILTRATION

Almost all the latest pieces of malware and attacks have data exfiltration capabilities and the information security world is facing big challenges to stop them. As previously said, at the moment data exfiltration is applied by making use of renown classical methods, but they can be detected by properly tuned *IDSs*. In this work, we present a tool that uses *PBT* for data exfiltration. Moreover, we evaluate the tool against the most common and widely used *IDSs* to test what they are able to detect and under which circumstances.

We assume a scenario where we are able to infect a machine inside the private network without detection from the security administrator. Hence, we study the scenario after the infection. We mainly focus the study on the Network Intrusion Detection Systems *(NIDS)* due to the polymorphic blending technique we intend to use, which is specifically designed to evade network-monitoring systems. In this scenario, sensitive data is represented by confidential files stored in the infected machine. Everything with access to the machine has also access to these files. Finally, we assume that our view of the network is consistent with the IDS' view. This means that the tool must have enough permissions to be able to sniff on the local interface. Otherwise it cannot collect the traffic information.

A. The Exfiltration Tool

The goal of the exfiltration tool is to send data from a compromised machine to a remote server, which is outside the compromised network and under the control of the attacker, while avoiding the security measures that may be in place. In this particular case, these security measures are represented by the *IDS*s. The exfiltration tool is composed of two main entities: *the collector and the blender*. The data is sent to an external part of the tool called *BlackHole*. It identifies the drop-zone of the malware, which is where all the exfiltrated data is collected. The structural design of the tool is represented in Figure 2.

The collector collects network traffic by sniffing on the local network interface and it stores the statistics on a shared *statistic table*. The collected features are described in Figure 3 and they are divided by the three different layers of extraction such as *transport, payload* and *host*. The general tag describes whether the feature is common for every connection or depending on the single one.

FIGURE 2: TOOL ARCHITECTURE

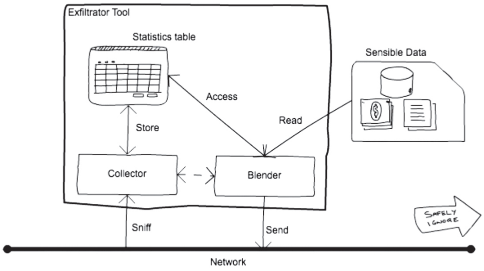
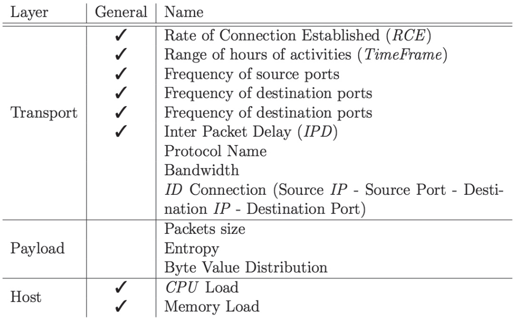


FIGURE 3: TRAFFIC FEATURES



Layer	General	Name
Transport	✓	Rate of Connection Established (*RCE*)
	✓	Range of hours of activities (*TimeFrame*)
	✓	Frequency of source ports
	✓	Frequency of destination ports
	✓	Frequency of destination ports
	✓	Inter Packet Delay (*IPD*)
		Protocol Name
		Bandwidth
		ID Connection (Source *IP* - Source Port - Destination *IP* - Destination Port)
Payload		Packets size
		Entropy
		Byte Value Distribution
Host	✓	*CPU* Load
	✓	Memory Load

The statistic table contains data that is continuously updated as well as features for completed connections. For every new connection, the collector stores the statistics and the byte distribution of the single connection to a temporary table and only when the connection is closed this data is moved to the statistics table. The statistic table is implemented as a hash table and it represents the network profile in the tool.

The blender is in charge of the real exfiltration. It sends out sensitive data shaping the traffic according to the normal profile calculated by the collector. Observing the statistics, it checks whether the right conditions for the exfiltration are satisfied: for example, it controls if the time frame allows new connections or if the workload of the infected machine is below a suspicious threshold. If the number of closed connections stored in the statistic table is above a certain threshold, we can start the exfiltration otherwise we wait. It selects a connection from the statistics table that has the entropy as close as possible to the file to exfiltrate, and then it starts to exfiltrate. The blender supports three different obfuscation methods: *XOR, Cesar13*[1], or byte substitution. For the first two methods, the blender applies basic obfuscation without extra traffic manipulation and they are used only for the sake of the tests. The first packet the blender sends to the server is the conversion table which is the table used to deobfuscate the following packets. The conversion table contains the type of obfuscation used: in case of *XOR*, it contains only the obfuscation key, on the contrary in case of byte substitution, it contains the decryption table which is the reversed byte mapping table to be used for the deobfuscation. The byte mapping table or encryption table is created by combining the selected connection with the file byte distribution, so that the most used byte in the file is mapped with the most used byte in the connection. The blender sends the sensitive data in chunks, each of them obfuscated and respecting the traffic statistics of the selected connection. In fact, the blender also sends the packets with the same bandwidth and the same packet size of the connection, so as it is able to exfiltrate data by imitating the recorded traffic.

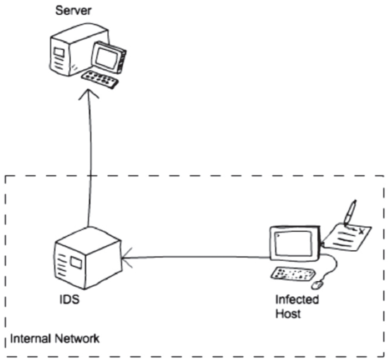
The *BlackHole* is the external entity used by the tool to drop the exfiltrated file. It runs one *TCP* and one *UDP* server and it waits for a transmission to begin. It just needs the first packet with the deobfuscation information in order to perform its task, which is to receive and reconstruct the file.

B. Test Environment

We tested our tool against the following most used *IDSs* divided per type: as signature-based *IDS* we used *Snort (Version 2.9.2 IPv6 GRE (Build 78))*[21], as anomaly-based *IDS* we used *SnortAD (Version 2.9.2.3 IPv6 GRE (Build 205) and AnomalyDetection Version 3.1)* [22] and *McPAD* (site version) [8], and finally as hybrid solution we used *Suricata (Vesion 2.0.2)* [23] and *Bro (Version 2.3-124)* [24]. These were used with the default configurations. I only added the signatures of the sensitive files for Snort and Suricata. They were created by using the first bytes of each sensitive file, which identify the type. For the *anomaly-based IDS*, the profile was created by using from 5 to 10 days of traffic recording. It was normal traffic recorded during a working day then repeated many times. This is the same traffic used to train the Collector.

[1] The classic *Cesar13* (or *Rot13*) encryption is limited to alphabet characters so in our work we implemented an extended version which uses all the 256 UNICODE characters. In the whole paper this extended version will be referred as *Cesar13*.

FIGURE 4: EXFILTRATION ENVIRONMENT



The test was conducted in an artificial environment as represented in Figure 4. The *IDS* in figure is configured as network gateway, so all the traffic coming from the client goes through the *IDS*. It listens to the internal interface sniffing all the traffic. The client using *tcpreplay* replayed the recorded traffic, which was used to train the *IDS* as well as during the execution of the tool.

C. Evaluation

During the evaluation, we wanted to test the detection capabilities of different *IDSs* against exfiltration and especially exfiltration using *PBT*. For this purpose, we selected different types of files to act as sensitive files in order to be more realistic in our tests. They are listed in Figure 6 along with their entropy.

FIGURE 5: EXFILTRATION TIME PER SENSITIVE FILE USING PBT

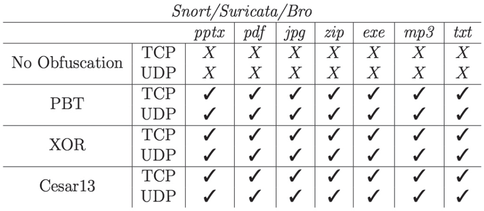
Type	Size (Byte)	Exfiltration time	Normal Transfer
pptx	3.6M	6.81 min	1.0 sec
jpg	98K	10.98 sec	0.3 sec
pdf	1.7M	3.1 min	0.8 sec
zip	210K	3.6 min	0.4 sec
mp3	3.4M	6.43 min	0.9 sec
exe	2.8M	40.56 min	0.9 sec
txt	19K	16 sec	0.1 sec
iso	911M	30.11 hours	90.4 sec

FIGURE 6: SENSITIVE FILES

Type	Size (Byte)	Entropy	Entropy Scale
pptx	3.6M	0.99911088065	HIGH
jpg	98K	0.997354080948	HIGH
pdf	1.7M	0.996589737052	HIGH
zip	210K	0.985803020077	MEDIUM
mp3	3.4M	0.982546526443	MEDIUM
exe	2.8M	0.873447456656	LOW
txt	19K	0.723637261467	LOW

During the tests, we exfiltrated all types of files using all the three obfuscation techniques. *XOR* and *Cesar13* do not perform any traffic manipulation, it is only implemented by *PBT*. We were able to exfiltrate our testing sensitive files within one hour time. We also tested the exfiltration of a larger file (around *911Mb*) taking around *30* hours. Figure 5 shows the detailed exfiltration time per file, even though it is important to emphasize that these times are strongly dependent on the traffic profile and on the connection selected in the profile. These times are only related to *PBT* exfiltrations. We wanted to test the ability of an *IDS* to detect an exfiltration, so our results are expressed in terms of success (✓) when the *IDS* raised an alert in front of an exfiltration, failure (×) otherwise.

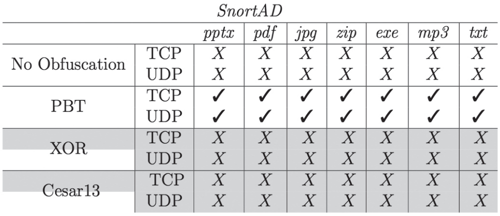
FIGURE 7: EXFILTRATION WITHOUT DETECTION WITH SNORT, SURICATA, AND BRO.



Snort/Suricata/Bro

		pptx	*pdf*	*jpg*	*zip*	*exe*	*mp3*	*txt*
No Obfuscation	TCP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
	UDP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
PBT	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
XOR	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
Cesar13	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓

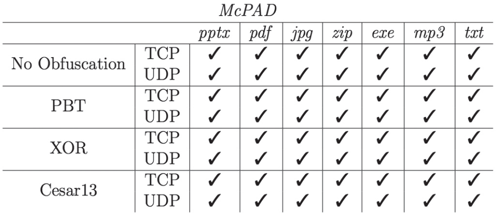
FIGURE 8: EXFILTRATION WITHOUT DETECTION WITH SNORTAD.



SnortAD

		pptx	*pdf*	*jpg*	*zip*	*exe*	*mp3*	*txt*
No Obfuscation	TCP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
	UDP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
PBT	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
XOR	TCP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
	UDP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
Cesar13	TCP	*X*	*X*	*X*	*X*	*X*	*X*	*X*
	UDP	*X*	*X*	*X*	*X*	*X*	*X*	*X*

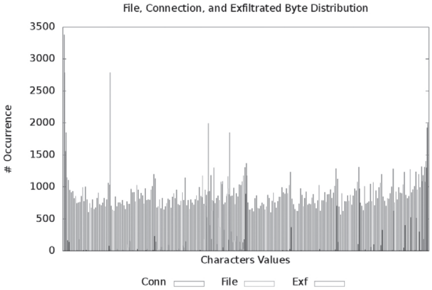
FIGURE 9: EXFILTRATION WITHOUT DETECTION WITH MCPAD.



McPAD

		pptx	*pdf*	*jpg*	*zip*	*exe*	*mp3*	*txt*
No Obfuscation	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
PBT	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
XOR	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓
Cesar13	TCP	✓	✓	✓	✓	✓	✓	✓
	UDP	✓	✓	✓	✓	✓	✓	✓

FIGURE 10: BYTE DISTRIBUTION WITH EXFILTRATTED TRAFFIC.



Snort and *Suricata* were able to detect only not obfuscated exfiltrations as shown in Figure 7 since, as it could be expected, signature-based *IDSs* failed against any form of obfuscation. Even with *Bro* we had the same results (Figure 7). In fact, we could not find any feature in the exfiltration that could stand out such that they could be described in its very advanced scripting language.

SnortAD increases the rate of detected exfiltrations as shown in Figure 8. Since the obfuscation using *XOR* and *Cesar13* does not apply any kind of blending, they are easily spotted by the *IDS*. In fact, when blending is applied, beside the payload other traffic features are modified by changing the shape of the traffic. *SnortAD* is able to detect every exfiltrations we tested, except those using *PBT*. With *PBT*, we calculated the byte distribution and we applied byte substitution according to it. The exfiltrated traffic byte distribution is shown in Figure 10 compared with the ones of the connection and the file. As we can see, the exfiltrated data (blue bars) has the same byte distribution of the connection (red bars) but with the same number of bytes occurrences of the file (green bars). The tests performed on *SnortAD* were also able to select the most effective traffic feature that permits the detection: the bandwidth. In fact, by tweaking the bandwidth we were able to fix *30%* as the threshold within which the bandwidth can fluctuate without producing detection.

All the *IDSs* performed as expected with the exception of *McPAD*. It produced no detection in all the tests performed as shown in Figure 9. It has been fed with the same traffic profile we provided to *SnortAD* but in this case it was not useful. The reason for the *McPAD* behaviour is that it has too narrowed capabilities. Even though there are configurable parameters, they do not allow to specify any extra rules able to detect our traffic. We placed this *IDS* with the same condition of all the others but it was the only one that did not produce any detection and so we can conclude that it is not fit for the task. In fact, our technique removes the invariant of the decryption code always present in few bytes of the packets of the PBA, those specific bytes that help *McPAD* for detection.

5. COUNTERMEASURE

We successfully proved that *PBT* is able to exfiltrate sensitive data, while avoiding detection of the most common and widely used *IDSs*. Unfortunately, this technique is not bullet proof: by improving the *IDS* detection engine we can be able to detect also our technique. For example, we can improve the anomaly-based *IDS* combining the information of the number of packets in a time frame with the concept of flow. For example, when the *IDS* collects the statistics about the normal traffic we can detect the average, the max, and the min of the data exchanged within the same flow (*TCP* or *UDP*), and the number of time frame used by an active flow. By using this information, our exfiltration can be detected because of three reasons: the flow goes over a long time, the flow is always active, and the amount of data is of considerable size for a single flow. Moreover, we have an exposed point in our exfiltration: the first packet. We transmit crucial information for the exfiltration in the first packet and we do it in clear. When using byte substitution, this packet contains the decryption table that, in most cases, it is *512* bytes big. Consequently, we can create a signature of such packet for the *IDS* so that it can be able to detect the exfiltration from the beginning. Unfortunately, even though it can be a useful alert, this signature is too generic and it can produce too many false positive. In fact, we cannot make any assumption about the content of the packet since it changes completely every time, and it depends on both the selected connection and the file to be exfiltrated.

Such is the well-known discussion always present in security: the *Achilles and the Tortoise* paradox of security. We are witnesses of defenders and attackers running after each other. Even in this case this scenario applies perfectly. Improving the *IDS* with the previously described features does not stop the exfiltration to adjust the shot. The improved *IDS* can be easily evaded by our exfiltration by using multiple connections for a single exfiltration or by using multiple drop zones. In this way, the single flow is shorter and it is transmitting a smaller amount of data. The exfiltration can also be spread over a longer time just by stopping and restarting the connection in different time frames. Lastly, the exfiltration can also be improved by removing the single of point of failure of the first unobfuscated packet. Since it is relatively small (only *512* bytes), it can be transmitted using back channels such as *DNS tunnelling* without being suspicious and attracting any attention.

While all these improvements can be considered reasonable, they have not been tested yet and we consider this as part of future works.

As we can see, the *PBT* results a really effective technique due to its capacity of imitating whatever is considered legitimate traffic, while it makes the detection by *IDSs* almost impossible.

6. CONCLUSION

Data leakage represents a major threat for companies and states, so the attention is moving more and more on studying exfiltration technique. Gradually, the crucial aspect is to find solutions able to detect the exfiltrations. Signature-based *IDSs* can detect exfiltrations if they do not use any kind of obfuscation. As soon as even the most classical obfuscation method is used, *SIDSs* are not able to detect them anymore. Only the more advanced anomaly-based *IDSs* can be up to the task. Those are able to detect exfiltrations that use normal obfuscation methods.

In this work, we exfiltrated data by using the more advanced Polymorphic Blending Technique in order to avoid detection. We implemented this technique along with other obfuscation method in a tool capable to exfiltrate sensitive data from an infected machine to a server controlled by the attacker.

The tool is used to test the detection capabilities of different type of *IDSs* against exfiltration. Using the *PBT*, the tool is able to successfully exfiltrate any type of file evading our selection of the most used *IDSs*. Even the more advanced anomaly-based *IDSs* cannot detect such type of exfiltration.

Finally, we calculated 30% as exfiltration threshold within which the tool can perform a safe exfiltration exploiting the *IDSs* tolerance.

7. FUTURE WORKS

The tool we have implemented represents a proof of concept used to test the detection capabilities of the *IDSs*. It implements the really basic functionalities necessary to perform exfiltration and it can be extended with many more capabilities. For example, it can implement the detection countermeasures described in Chapter 5. Moreover, the tool applies only manipulation of the traffic features but it does not use any other evasion techniques [25] such as fragmentation or session manipulation. This could be a different front where to test the *IDSs*.

Finally, we limited our tests to a subset of *IDSs* but it would be interesting to test the tool against other *IDSs* such as *ExFILD* [15].

REFERENCES

[1] R. Van Antwerp, "Exfiltration techniques: An examination and emulation" PhD Thesis, University of Delaware, 2011.

[2] S. Axelsson, "Intrusion Detection Systems : A Survey and Taxonomy" Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2000.

[3] A. Giani, V. H. Berk, and G. V Cybenko, "Data exfiltration and covert channels," in Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V. Edited by Carapezza, Edward M. Proceedings of the SPIE, 2006, vol. 6201, p. 620103.

[4] J. Andress and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 1st ed. Syngress Publishing, 2011.

[5] G Data SecurityLabs, "Uroburos Highly complex espionage software with Russian roots" Technical Report G Data SecurityLabs, 2014.

[6] F-secure Labs Security Responce, "COSMICDUKE: Cosmu with a twist of MiniDuke" Technical Report F-secure Labs, 2014.

[7] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic blending attacks" in Proceedings of the 15th USENIX Security Symposium, 2006, pp. 241–256.

[8] R. Perdisci, D. Ariu, P. Fogla, G. Giacinto, and W. Lee, "McPAD: A multiple classifier system for accurate payload-based anomaly detection" Comput. Networks, vol. 53, no. 6, pp. 864–881, 2009.

[9] I. I. Amit, V. P. Consulting, and S. Art, "Advanced Data Exfiltration – the way Q would have done it" GovcertNT, Rotterdam, Netherlands, 2011.

[10] S. Wendzel, W. Mazurczyk, L. Caviglione, and M. Meier, "Hidden and Uncontrolled-On the Emergence of Network Steganographic Threats" arXiv Prepr. arXiv1407.2029, 2014.

[11] S. Wendzel, "Novel Approaches for Network Covert Storage Channels" PhD Thesis, Fernuniversität Hagen, 2013.

[12] F. V. Yarochkin, S. Y. Dai, C. H. Lin, Y. Huang, and S. Y. Kuo, "Towards adaptive covert communication system" Proc. 14th IEEE Pacific Rim Int. Symp. Dependable Comput. PRDC 2008, pp. 153–159, 2008.

[13] S. Khattak, M. Javed, P. D. Anderson, and V. Paxson, "Towards Illuminating a Censorship Monitor's Model to Facilitate Evasion," Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet, Berkeley, CA, pp. 1–7.

[14] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications" in Security and Privacy (SP), 2013 IEEE Symposium on, 2013, pp. 65–79.

[15] T. Fawcett, "ExFILD: A tool for the detection of data exfiltration using entropy and encryption characteristics of network traffic" PhD Thesis, University of Delaware, 2010.

[16] D. Bolzoni, B. Crispo, and S. Etalle, "ATLANTIDES: Automatic Configuration for Alert Verification in Network Intrusion Detection Systems" In: LISA '07: Proc. 21th Large Installation System Administration Conference, USENIX Association (2007) 141–152.

[17] B. Guttman and E. A. Roback, An introduction to computer security: the NIST handbook. DIANE Publishing, 1995.

[18] A. Rashid, R. Ramdhany, M. Edwards, S. M. Kibirige, A. Babar, D. Hutchison, R. Chitchyan, "Detecting and Preventing Data Exfiltration" Technical Report, Academic Centre of Excellence in Cyber Security Research, 2014.

[19] M. Van Horenbeeck, “Deception on the network: thinking differently about covert channels” School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2006.

[20] W. Mazurczyk, “VoIP steganography and its Detection—A survey,” ACM Computer Survey, vol. 46, no. 2, p. 20, 2013.

[21] M. Roesch and others, “Snort: Lightweight Intrusion Detection for Networks” in LISA, 1999, vol. 99, pp. 229–238.

[22] M. Szmit, R. Wezyk, M. Skowro’nski, and A. Szmit, “Traffic Anomaly Detection with Snort” Information Systems Architecture and Technology. Information Systems and Computer Communication Networks, Wydawnictwo Politechniki Wrocławskiej, Wrocław, pp. 181–187, 2007.

[23] D. Day and B. Burns, “A performance analysis of snort and suricata network intrusion detection and prevention engines” in ICDS 2011, The Fifth International Conference on Digital Society, 2011, pp. 187–192.

[24] V. Paxson, “Bro: a System for Detecting Network Intruders in Real-Time” Computer Networks, vol. 31, no. 23–24, pp. 2435–2463, 1999.

[25] K. Timm, “Ids evasion techniques and tactics” SecurityFocus (Infocus), vol. 7, 2002.

2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Attacking the Baseband Modem of Mobile Phones to Breach the Users' Privacy and Network Security

Christos Xenakis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
xenakis@unipi.gr

Christoforos Ntantogian
Department of Digital Systems
University of Piraeus
Piraeus, Greece
dadoyan@unipi.gr

Abstract: As people are using their smartphones more frequently, cyber criminals are focusing their efforts on infecting smartphones rather than computers. This paper presents the design and implementation of a new type of mobile malware, named (U)SimMonitor for Android and iPhone devices, which attacks the baseband modem of mobile phones. In particular, the mobile malware is capable of stealing security credentials and sensitive information of the cellular technology including permanent and temporary identities, encryption keys and location of users. The developed malware operates in the background in a stealthy manner without disrupting the normal operation of the phone. We elaborate on the software architecture of (U)SimMonitor and provide implementation details for the specific AT commands used by the malware. We analyse the security impacts of (U)SimMonitor malware and we show that it can entirely breach the privacy of mobile users and the security of cellular networks. In particular, a mobile user with an infected phone can be identified and all his/her movements can be tracked. Moreover, all his/her encrypted phone calls and data sessions can be disclosed.

Keywords: *mobile malware, mobile networks, android, iPhone, AT commands*

1. INTRODUCTION

Cellular networks have been continuously evolving to support high data rates and provide internet access that can fulfil the demands of today's web applications [1]. Along with cellular networks, the mobile phones are also evolving to smartphones with processing capabilities and storage resources that are often equivalent to contemporary personal computers. The potential of smartphones is leveraged by mobile operating systems, such as iOS and Android OS that allow end-users to access traditional desktop applications using these portable devices. Along with the variety of new perspectives, smartphones also raise new security concerns and issues. In particular, due to their popularity, smartphones have become prime targets for malware. In 2013, 3.905.502 installation packages were used by cyber criminals to distribute mobile malware [2].

The majority of mobile malware aims at causing financial charges to infected mobile phones. For example, sending SMS messages to premium-rate numbers without the users' consent is a usual malicious activity of a mobile malware. These numbers can be either hardcoded in the malware code or downloaded at runtime to avoid detection. Other types of mobile malware collect sensitive data from the infected phone including SMS messages, phone numbers, email addresses and username/passwords from applications. Moreover, some infected phones are turned into bots for HTTP-based remote control by a botmaster. In general, we can observe that mobile malware target and exploit the characteristics of the mobile OS to perform a variety of malicious actions [3]. To the best of our knowledge, there is no mobile malware that targets the baseband modem of mobile phones to breach the privacy of mobile users and the security of cellular networks.

This paper presents the design and implementation of a new type of mobile malware, named (U)SimMonitor for Android and iPhone devices, which attacks the baseband modem of mobile phones. In particular, it is a mobile malware capable of stealing security credentials and sensitive information of the cellular technology (i.e., permanent and temporary identities, encryption keys, location of users, etc.) and profoundly compromising the privacy of users and the mobile network security. The developed malware (i.e., (U)SimMonitor) operates in the background without the victim user noticing its existence, since it does not disrupt the normal operation of the phone. We elaborate on the software architecture of (U)SimMonitor and provide implementation details for the specific AT commands used by the malware. We analyse the security impacts of (U)SimMonitor malware and we show that it can entirely breach the privacy of mobile users and the security of cellular networks. In particular, a mobile user with an infected phone can be identified and all his/her movements can be tracked. Moreover, all his/her encrypted, by the cellular technology, phone calls and data sessions can be disclosed. The criticality of this malware is evident: it eliminates the need of breaking the security of the employed cryptographic algorithms, since the encryption keys are in the possession of the attacker. Thus, this malware comprises a threat for all mobile networks technologies, even for the security-enhanced long term evolution (LTE) networks, since it renders inadequate all possible security measures that can be employed in cellular networks. We believe that mobile antivirus products should update their signatures to detect (U)SimMonitor malware and its variants. Overall the contributions of this paper are:

- Identify and analyse the security criticality of a new type of mobile malware named (U)SimMonitor, which is capable of stealing security credentials and sensitive information of mobile users and cellular networks and profoundly compromising the privacy of users and the network security.
- Design and implementation of the (U)SimMonitor that proves the feasibility of this new attack vector.
- Release the source code of (U)SimMonitor and practical demonstration.

The remainder of this article is organized as follows. Section 2 presents briefly the cellular network technology and the related work. Section 3 presents the design and implementation of (U)SimMonitor. Section 4 elaborates on the security impacts of (U)SimMonitor and how it can entirely breach the privacy of users. Finally, section 5 concludes the article.

2. BACKGROUND

A. Cellular Network Technology and Android

Cellular networks are composed of various interworking technologies including 2G and 3G networks [4]. A basic element of cellular networks is the mobile station (MS), which enables a user to connect to a serving network and enjoy services. MS includes the user's equipment (UE) and a subscriber's service identity module (SIM) or UMTS SIM (USIM) card. The latter is an integrated circuit that stores various parameters of the mobile network, including the international mobile subscriber identity (IMSI), which is the permanent identity of a subscriber in a mobile network as well as encryption and integrity keys.

The UE of MS is a smartphone that runs a mobile OS. The most prominent mobile OS is Android having an 81% market share in the third quarter of 2013 [5]. Android applications are implemented with Java programming language and executed in their own virtual machine named Dalvik. The latter relies on the Linux kernel for the underlying OS functionality, such as threading and low-level memory management. Typically, in a smartphone there are two processors: the application processor that is used to run Android OS and the baseband modem processor, where all the radio operations take place. In modern phones, these processors and all other peripheral devices are integrated into one piece of hardware (i.e., System on a Chip (SoC)).

B. Related Work

The related work in this research area focuses mainly on the defensive side, proposing solutions that detect or prevent mobile malware from infecting mobile devices. In particular, several works propose security enhancements in mobile platforms that perform fine-grained access control of system resources when they are accessed by untrusted third party applications [3]. Moreover, many past works put their efforts in detecting mobile malware by applying machine learning algorithms [6].

On the other hand, there are very few papers that elaborate on AT commands and their important functionality in mobile phones. In the work closest to ours [7], the authors analyse theoretically the potential of cellular botnets that can perform a coordinated and distributed denial of service (DDoS) attack to a Home Location Register/Authentication Centre (HLR/AuC). The analysed DDoS attack is performed by a malware that can initiate appropriate AT commands that trigger network-oriented activities (e.g., location update). However, the authors have overlooked to analyse the specific AT commands that are required to perform the proposed DDoS attack. Moreover, the authors do not elaborate on the design and implementation of the mobile malware to perform AT commands. Thus, the feasibility of this malware and the related DDoS attack is not proved.

In our previous work [8], we have presented an advanced persistent threat (APT) in 3G networks that exploits a series of zero-day vulnerabilities to flood the HLR/AuC, leading to system saturation. It was proven that the discovered APT can be performed in a trivial manner using commodity hardware and software. To this end, a mobile application was implemented that performs continuous network registrations using AT commands. The application uses the dial command to initiate phone calls using a different IMSI for each call request. This was achieved using a device named simtrace [9], which acts as an active man in the middle between the modem and SIM/USIM card and can change the IMSI identity when it is requested by the modem.

In [10], the authors utilize AT commands from a different point of view: that is, they use AT commands in order to perform SMS fuzzing for iPhone, Android and Windows mobile phones. Their goal was to discover previously unknown software bugs in SMS applications that can be exploited by malicious actors to perform DoS attacks. The authors successfully discovered a set of critical bugs in both iOS and Android SMS applications. Moreover, [11] analyses the design and implementation of a passive man-in-the-middle application for iOS and Android phones that listens the communication between the radio interface layer (RIL), which is a software middleware that controls modem through AT commands, and the modem. In this way, [11] achieved to log all the invoked AT commands by the RIL and the modem during phone calls, SMS sending/receiving, etc. Apart from these works, we have discovered a free online tool named AT command tester [12], which is implemented in Java, and allows the execution of a comprehensive set of AT commands to GSM modules via a web browser.

Finally, we mention here that there are many commercial and free mobile applications for Android and iPhone devices such as [13] that can listen and record voice calls or even stream in real time the intercepted calls to the malicious actor. (U)SimMonitor is a new, alternative way to intercept phone calls by targeting the baseband modem and extracting the GSM and 3G encryption keys. Thus, the proposed malware is not only able to decrypt voice calls, but also the Internet traffic of the victim.

3. (U)SIMMONITOR

A. Overview

In this section we present and analyse the architecture and the key functionality of (U)SimMonitor for the Android OS. Implementation details are presented in [14], while the source code of (U)SimMonitor can be found in [15]. It is important to mention that we have also developed successfully a similar malware application for the iOS operating system of iPhones. The main purpose of (U)SimMonitor is to extract security related data from SIM and USIM cards [16]. To achieve this, it communicates with the modem of the mobile phone through a set of AT commands. This procedure is executed, periodically, at specific time intervals or based on various events, as analysed below. (U)SimMonitor stores the fetched data from the modem in a local database on the phone and periodically or on-demand it uploads the stored data to a server for further processing and analysis. The malware runs in the background, while the user can normally operate his/her phone. To this end, the (U)SimMonitor uses the least possible resources of the modem, in order to avoid blocking accidently a voice/data communication. In general, (U)SimMonitor has been designed to collect data transparently, without disrupting the proper operation of the phone. Thus, it can hide its malicious activities and avoid detection, due to its stealthy nature.

Moreover, (U)SimMonitor stops and restarts the RIL daemon when it executes an AT command to avoid possible disruptions from the Android. More specifically, the functionality of the RIL daemon is to provide the interface that handles the communication between the Android phone framework services and the radio hardware [17]. During our tests, we observed that initially (U)SimMonitor was not able to communicate directly with the modem through AT commands. After investigation, we discovered that some vendors implement RIL in a way that the modem is able to respond only to one process at a time. For this reason, the (U)SimMonitor could not execute AT commands to the modem, since the latter was always in use by Android. To overcome this limitation, the (U)SimMonitor incorporates a payload that stops the RIL daemon before initiating the execution of AT commands and restarts it immediately after the modem responds to the last AT command. We remark here that during our experiments and usage of the (U)SimMonitor, the normal operation of the phone was not affected by stopping and starting the RIL daemon, since this procedure (i.e., restarting the RIL daemon) is executed in under one second (<1 sec) without the user receiving any notification.

Apart from its main functionality (i.e., extracting security data), the (U)SimMonitor incorporates a dropper payload for privilege escalation. More specifically, for security reasons, Android and iOS do not allow the execution of applications with root permissions. However, (U)SimMonitor is able to execute AT commands only if it has root privileges. To overcome this restriction, (U)SimMonitor includes a dropper payload, which essentially downloads binary code that exploits known vulnerabilities in Android and iOS, in order to elevate privileges. The downloaded exploitation code is obfuscated, in order to avoid detection from mobile AV [18].

B. AT Commands

AT commands lie at the core of (U)SimMonitor providing various operations to control a modem, as specified in 3GPP TS 27.007 [19]. Based on the provided functionality, AT commands can be categorized as follows:

- Call control: commands for initiating and controlling calls.
- Data call control: commands for controlling the data transfer and the Quality of Service (QoS).
- Network services control: commands for supplementary services, operator selection, locking and registration.
- SMS control: commands for sending, notifying of received SMS messages, and configuring SMS services.
- Data retrieval: commands to obtain information for the subscriber and the phone, such the IMSI, the IMEI, radio signal strength, batter status. etc.

The (U)SimMonitor makes extensive use of the last category of AT commands (i.e., data retrieval) to extract security related data from the SIM/USIM. A summarizing list of the AT commands, which we used to obtain security related data as well as their proper syntax, is presented in Appendix. In all our testing mobile devices we have successfully installed and executed (U)SimMonitor. These devices are:

- Samsung S-5500
- Samsung S-6500
- Samsung Galaxy s2
- ZTE Blade
- HTC Sensation XE with Beats Audio
- Sony Ericsson Xperia LT18i

C. Data Collection

(U)SimMonitor collects sensitive and security related data [20] [21], which are extracted through AT commands. These data are briefly presented below:

IMSI: The international mobile subscriber identity (IMSI) is a unique number permanently associated to the holder of the SIM/USIM card. Its size is 8 bytes. The first three bytes of IMSI represent the mobile country code (MCC), while the next two or three bytes represent the mobile network code (MNC). The remaining bytes represent the mobile subscriber identification number (MSIN).

K_c: A 64-bit ciphering key used to encrypt voice and data communication between the MS and BTS of GSM networks [22].

K_{cGPRS}: A 64-bit ciphering key used to encrypt communication data between the MS and the SGSN of GPRS networks.

CK: A 128-bit ciphering key used to encrypt the communication between the MS and the RNC of UMTS.

IK: A 128-bit key to protect the integrity of the signalling data between the MS and the RNC of UMTS network.

Threshold: A 24-bit value which represents the lifetime of the CK and IK keys in UMTS networks.

Ciphering Indicator: This is a 1-bit flag that allows the MS to detect whether ciphering is switched on (flag set to 1) or off (flag set to 0). The ciphering indicator feature may be disabled by the mobile network operator.

TMSI: The temporary mobile subscriber identity (TMSI) is a temporary identity of MS, which is assigned from the mobile network and it is used instead of IMSI for enhancing anonymity. TMSI is valid for circuit switching (CS) domain and its size is 4 bytes.

TMSI Time: This is a 1 byte value and represents the maximum time interval which the assigned TMSI can be used.

P-TMSI: The packet TMSI (P-TMSI) is the complement of TMSI in the UTRAN/GERAN packet switching (PS) domain.

P-TMSI Signature value: This is a signature used by the 3G network for verifying the validity of P-TMSI of MS. Its size is 3 bytes.

LAI: The location area identity (LAI) is a 5 bytes unique identifier for each location area in the CS domain. It consists of MCC, MNC and the location area code (LAC).

RAI: The Routing Area Identity for PS domains is the analogous to the LAI for CS domains. RAI consists of LAI (which is 5 bytes) and a 1 byte Routing Area Code.

Provider: This is the name of the mobile network operator.

Cell Id: This is the unique identity of the cell tower, where the MS is connected at the moment of data collection.

Network type: This parameter indicates the mobile network technology, where the MS is connected, at the moment of data collection. It may have several values including GPRS, EDGE, UMTS, HSDPA, LTE, UNKNOWN, etc.

Roaming: A 1-bit value that indicates whether MS is outside the coverage area of its home network.

Moreover, (U)SimMonitor collects some additional metadata as mentioned below:

Event Type: This value indicates the event that triggered the data collection. The possible event types are: i) Outgoing or incoming calls, ii) Screen on or off, iii) Power on or off, iv) Periodic (i.e., a time interval where data is collected periodically).

Latitude, Longitude: These values are the coordinates of the geographical position of MS at the moment of data collection. The coordinates are determined either by the GPS sensor of the phone or the Wi-Fi signals.

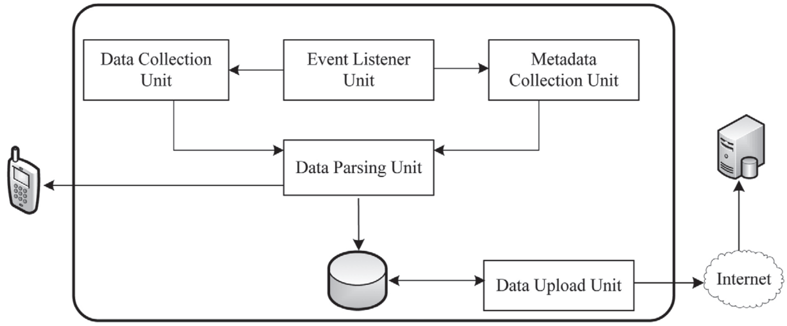
Timestamp: The date and time of data collection.

D. Software Architecture

As shown in figure 1, the software architecture of (U)SimMonitor consists of five units, each one undertaking a specific task. More specifically, these units are as follows:

1. Metadata collection
2. Event listener
3. Data collection
4. Data parsing
5. Data upload

FIGURE 1: (U)SIMMONITOR APPLICATION ARCHITECTURE



The event listener unit monitors and captures the occurrence of an event. Possible event types are: i) Outgoing or incoming calls, ii) Screen on or off, iii) Power on or off, iv) Periodic (i.e., a time interval where data is collected periodically). When one of these events occurs, the event listener unit triggers the metadata collection and data collection units. The metadata collection unit obtains the coordinates of the smartphone using the GPS sensor or Wi-Fi signals as well as the time that data extraction occurred. On the other hand, the data collection unit communicates with the modem executing AT commands. To achieve this, it creates a system process to invoke a Linux shell script. The latter communicates with the baseband modem by executing sequentially a set of AT commands. For each AT command, the baseband modem contacts to USIM/SIM to obtain the related data (see figure 2). After receiving the response of the last executed AT command, the data collection unit terminates the system process in order to save memory resources.

Both the data collection unit and the metadata collection units transfer the obtained data to the data parsing unit. The latter filters out unnecessary information and stores the final data in a local database. Optionally, the parsing unit can also display the final data in the phone's screen. Figure 3 shows an Android phone and an iPhone displaying extracted data using (U)SimMonitor. Finally, as its name implies, the upload unit transfers the database contents to a secure server via SSH and subsequently deletes the contents of the database to save memory space in the phone.

FIGURE 2: (U)SIMMONITOR EXECUTION FLOW

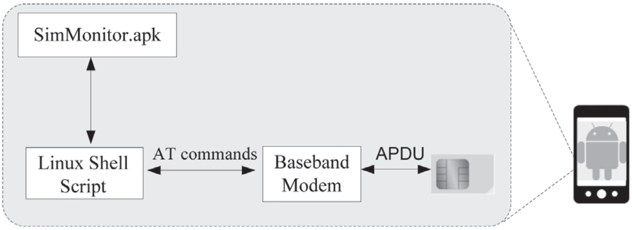
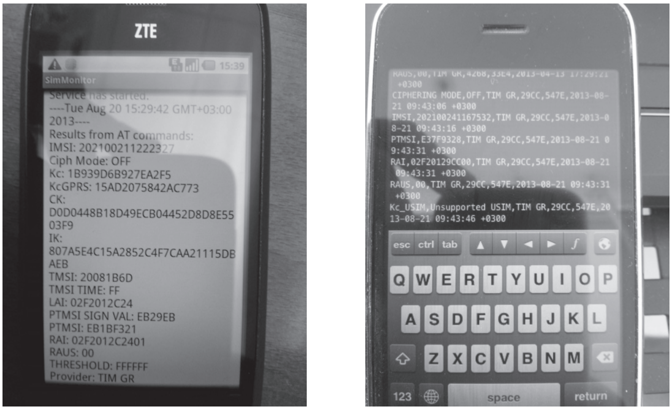


FIGURE 3: (U)SIMMONITOR DISPLAYING COLLECTED DATA IN ANDROID AND IOS



```
Service has started.
----Tue Aug 20 15:29:42 GMT+03:00
2013----
Results from AT commands:
IMSI: 202100211222327
Ciph Mode: OFF
Kc: 1B939D6B927EA2F5
KcGPRS: 15AD2075842AC773
CK:
D0D0448B18D49ECB04452D8D8E55
03F9
IK:
807A5E4C15A2852C4F7CAA21115DB
AEB
TMSI: 20081B6D
TMSI TIME: FF
LAI: 02F2012C24
PTMSI SIGN VAL: EB29EB
PTMSI: EB1BF321
RAI: 02F2012C2401
RAUS: 00
THRESHOLD: FFFFFF
Provider: TIM GR
```

```
RAUS,00,TIM GR,4268,33E4,2013-04-13 17:29:21
 +0300
CIPHERING MODE,OFF,TIM GR,29CC,547E,2013-08-
21 09:43:06 +0300
IMSI,202100241167532,TIM GR,29CC,547E,2013-0
8-21 09:43:16 +0300
PTMSI,E37F9328,TIM GR,29CC,547E,2013-08-21 0
9:43:31 +0300
RAI,02F20129CC00,TIM GR,29CC,547E,2013-08-21
 09:43:31 +0300
RAUS,00,TIM GR,29CC,547E,2013-08-21 09:43:31
 +0300
Kc_USIM,Unsupported USIM,TIM GR,29CC,547E,20
13-08-21 09:43:46 +0300
```

4. SECURITY IMPACTS

The (U)SimMonitor introduces a new type of mobile malware for Android and iPhone devices. In particular, it is able to steal security credentials and sensitive information of the cellular technology networks (i.e., IMSI, TMSI, keys, LAI, RAI, Cell Id, etc.) and profoundly compromise the privacy of users and the mobile network security. The malware (i.e., (U)SimMonitor) is capable of operating in the background without the victim noticing its existence, since it does not disrupt the normal operation of the phone. Thus, the (U)SimMonitor can hide its malicious activities and avoid detection, due to its stealthy nature.

An attacker first should entice his/her victims to install and execute (U)SimMonitor without their permission and without raising any suspicion. There are many ways an attacker can achieve this. For example, an attacker can inject malware from a PC to a mobile Device using the USB port [18] or through advertising banners embedded in mobile applications [23]. However, the most common way is by injecting the malware functionality into a legitimate Android or iPhone application (i.e., Trojan application). In particular, the attacker first locates and downloads a popular mobile application. Next, he/she re-package the application by enclosing also the functionality of (U)SimMonitor. This procedure is also known as binding and there are freely available tools to perform it [24]. Finally, he/she submits the infected application to third party application markets. Using social engineering techniques, the attacker can lure his/her victims to download and install the infected application into his/her mobile phone.

After activation of the (U)SimMonitor in the victim's phone, the malware reads security related and sensitive data from USIM/SIM card, including the encryptions keys used in the mobile network (Kc, KcGPRS, CK) together with the TMSI/IMSI identities, the network operator of the user, the Location/Routing area and the Cell ID. Note that the malware can also extract geographical coordinates using GPS, but in order to remain stealthy it may avoid this action. The extracted data is uploaded to a server, which is deployed from the attacker. At this point the attacker can perform the following malicious actions:

- He/she can easily identify the victim user, since he/she has obtained the IMSI and TMSI identities, while using the location/routing area and Cell-ID parameters he/she can approximately track victim's movements.
- Disclose phone calls and data session of the victim user using the obtained encryption keys (i.e., Kc, KcGPRS, CK), regardless of the strength of the employed cryptographic algorithm. It is evident that first the attacker should capture the mobile communications of the victim.

The security criticality of the malware is related to the fact that it eliminates the need of breaking the security of the employed cryptographic algorithms, since the encryption keys are in the possession of the attacker. Thus, this new generation of malware comprises a threat for all mobile network technologies, even for the security enhanced LTE networks, since it renders inadequate all possible security measures that can be taken from the mobile operator.

To further elaborate on the malware characteristics of the (U)SimMonitor, we tested five popular mobile antivirus (AV) products whether they are capable of recognizing it as a virus. In particular, we tested the following mobile AVs:

- Norton Mobile Security Lite
- Kaspersky Internet Security
- Avast Mobile Security & Antivirus
- TrendMicro Mobile Security
- Zoner AntiVirus Free

We installed the above AV applications in a Samsung Galaxy S3 mobile phone running Android OS 4.2. Prior to scanning, we updated the AVs with their latest virus database as of August 2014. Unfortunately, none of the tested AVs raised an alarm. This result comes as no surprise, since the detection capabilities of mobile AVs are far lower that their desktop counterparts [25]. Therefore, mobile AVs should update their signatures to identify pattern strings that include AT commands, as they are thoroughly presented in the Appendix.

We believe that (U)SimMonitor should be also viewed as a proof of concept for the hidden dangers lurking by rooting mobile phones. As mentioned in section 3.A, (U)SimMonitor incorporates an extra payload (i.e., dropper) to download exploit code, in order to elevate root-level privileges. However, (U)SimMonitor may bypass the execution of the dropper if the malware infects an already rooted device and automatically obtain root privileges. Nowadays, the rooting procedure seems to be a common practise among many smartphone owners. In fact, the rooting procedure in many phones has been simplified into a one-click procedure [26], which allows even non-technically aware users to perform rooting. On the one hand, rooting allows users to remove vendors' software and install newer versions of android OS. On the other hand, gaining root access also entails circumventing the security restrictions put in effect by the Android and iOS operating system. This last observation seems to be often overlooked. That is, many mobile phone owners are not aware the fact that by rooting their phones, they are exposed to more threats. Thus, by analysing the security impacts of (U)SimMonitor and its potential for new attacks, we believe that this work should be also viewed as a warning of the subtle security implications of rooting mobile devices.

Having access to all the security related information and parameters of a mobile subscriber connected to a cellular network, (U)SimMonitor cannot only be employed for malicious (i.e., black hat) usage. On the contrary, it can be used to capture and analyse the security policy that a cellular operator enforces i.e., the invocation and employment of the specified security measures to protect its users, a functionality which is currently missing from Android and iPhone devices [27]. In particular, the (U)SimMonitor can inform the mobile users if ciphering is disabled, how often the encryption keys are refreshed and how often the temporary identities are updated. In this way, mobile users can have a better view of the provided level of security, while security researches can perform a quantitative risk assessment for mobile networks.

5. CONCLUSIONS

In this paper we presented the design and implementation of a new type of mobile malware, named (U)SimMonitor for Android and iPhone devices. The malware targets the baseband modem of mobile phones and extracts security credentials and sensitive information from SIM/ USIM cards using AT commands. The malware compromises entirely the privacy of mobile users and the security of cellular networks. That is, after infection an attacker can perform the following malicious actions:

- Identification and tracking of victim's movements using the IMSI/TMSI identities as well as the location/routing areas and the Cell ID parameters.
- Disclosure of voice calls and data connections using the extracted encryption keys of 2G and 3G mobile networks.

The criticality of the malware is evident: it eliminates the need of breaking the security of the employed cryptographic algorithms, since the encryption keys are in the possession of the attacker. Thus, this new generation of malware comprises a threat for all mobile network technologies, even for the security enhanced LTE networks, since it renders inadequate all possible security measures that can be taken from the mobile operator. Finally, we believe that mobile AVs should update their signatures and heuristic algorithms to identify pattern strings that include AT commands.

6. APPENDIX

In this section we present the AT commands that the (U)SimMonitor uses to extract data from the (U)SIM card. AV products can use the syntax of the following AT commands as signatures for their virus databases.

The exact syntax of AT Commands depends on their type. We can recognize two main types of AT commands:

- Basic commands are AT commands that do not start with "+", such as D (Dial), A (Answer), H (Hook control), and O (Return to online data state).
- Extended commands are AT commands that start with "+" and their main functionality is to retrieve data from (U)SIM cards.

(U)SimMonitor uses AT commands from the second category (i.e., extended). In particular, the most useful and frequently invoked AT command of (U)SimMonitor is +CRSM, which extracts various mobile network parameters from (U)SIM cards. A generic format for the +CRSM command invoked by the (U)SimMonitor is the following one:

```
AT+CSRM=x, y, p1, p2, w
```

The value of parameter x indicates whether the command will write to or read data from SIM/ USIM card. Since the (U)SimMonitor only extracts data, the value of x is always equal to

“176”, which indicates a READ operation. The value of y is an identifier for the type of data that we want to extract from the SIM and USIM card. For example, the identifier of IMSI for SIM and USIM cards is the value “6F07”. The values of p1, p2 represent the high and low order offset respectively (in terms of number of bytes) from the beginning of the identifier that we want to read or write data. In (U)SimMonitor both values of p1, p2 were both equal to 0 indicating no offset. Finally, the value of w indicates the number of bytes that the specific AT command wants to read or write.

Apart from CSRM, (U)SimMonitor also uses the commands COPS to extract the name of the operator and CREG to extract the LAC and the Cell ID. In the following table, we provide the exact syntax of the AT commands as they are invoked by (U)SimMonitor and their respective functionality.

TABLE 1: AT COMMANDS USED IN (U)SIMMONITOR

Functionality	Storage location in SIM and USIM cards	AT command
1. Extraction of IMSI	Stored in 6F07 (decimal 28423) for SIM and USIM	(SIM/USIM) AT+CRSM=176,28423,0,0,3
2. Extraction of Ciphering Indicator	Stored in 6FAD (decimal 28589) for SIM and USIM	(SIM/USIM) AT+CRSM=176,28589,0,0,3
3. Extraction of Ciphering Key Kc	Stored in 6F20 (decimal 28448) for SIM and 4F20 (decimal 20256) for USIM	(SIM) AT+CRSM=176,28448,0,0,9 (USIM) AT+CRSM=176,20256,0,0,9
4. Extraction of Ciphering Key KcGPRS	Stored in 6F52 (decimal 28498) for SIM and 4F52 (decimal 20306) for USIM	(SIM) AT+CRSM=176,28498,0,0,9 (USIM) AT+CRSM=176,20306,0,0,9
5. Extraction of Ciphering Key CK and Integrity Key IK	Stored in 6F08 (decimal 28424), applied to USIM only	(USIM) AT+CRSM=176,28424,0,0,33
6. Extraction of TMSI, TMSI TIME and LAI	Stored in 6F7E (decimal 28542) for SIM and USIM	(SIM/USIM) AT+CRSM=176,28542,0,0,11
7. Extraction of PTMSI, PTMSI Signature Value, RAI and RAUS	Stored in 6F53 (decimal 28499) for SIM and 6F73 (decimal 28531) for USIM	(SIM) AT+CRSM=176,28499,0,0,14 (USIM) AT+CRSM=176,28531,0,0,14
8. Extraction of THRESHOLD	Stored in 6F5C (decimal 28508), applied to USIM only	(USIM) AT+CRSM=176,28508,0,0,3
9. Extraction of Provider	-	AT+COPS?
10. Extraction of Lac and Cell ID	-	AT+CREG?

REFERENCES

[1] M. Page, M. Molina and G. Jones, “The Mobile Economy 2013,” A.T.Kearney, London, 2013.

[2] V. Chebyshev and R. Unuchek, “Mobile Malware Evolution: 2013,” Kaspersky Lab ZAO’s SecureList, 24 February 2014. [Online]. Available: http://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/. [Accessed 02 April 2015].

[3] Y. Zhou and X. Jiang, “Dissecting Android Malware: Characterization and Evolution,” in *2012 IEEE Symposium on Security and Privacy (SP)*, San Fracisco, CA, 2012.

[4] C. Xenakis and L. Merakos, “Security in third Generation Mobile Networks,” *Computer Communications*, vol. 27, no. 7, pp. 638-650, May 2004.

[5] Strategy Analytics, “Android Captures Record 81 Percent Share of Global Smartphone Shipments in Q3 2013,” Strategy Analytics, 31 October 2013. [Online]. Available: http://blogs.strategyanalytics.com/WSS/post/2013/10/31/Android-Captures-Record-81-Percent-Share-of-Global-Smartphone-Shipments-in-Q3-2013.aspx. [Accessed 02 April 2015].

[6] B. Amos, H. A. Turner and J. White, “Applying machine learning classifiers to dynamic Android malware detection at scale,” in *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, Italy, 2013.

[7] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel and T. L. Porta, “On cellular botnets: measuring the impact of malicious devices on a cellular network core,” in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009.

[8] C. Xenakis and C. Ntantogian, “An advanced persistent threat in 3G networks: Attacking the home network from roaming networks,” *Computers & Security*, vol. 40, no. 1, pp. 88-94, February 2014.

[9] OsmocomBB, “Osmocom SIMTrace,” OsmocomBB wiki, 03 April 2013. [Online]. Available: http://bb.osmocom.org/trac/wiki/SIMtrace. [Accessed 02 April 2015].

[10] C. Mulliner and C. Miller, “Fuzzing the Phone in your Phone,” in *Black Hat USA 2009*, Las Vegas, Nevada, 2009.

[11] F. Sanglard, “Tracing the Baseband: Part1 and Part2,” Fabien Sanglard’s Website, 11 May 2010. [Online]. Available: http://fabiensanglard.net/cellphoneModem/. [Accessed 02 April 2015].

[12] M2MSupport.net, “AT Command Tester,” M2MSupport.net, 16 March 2014. [Online]. Available: http://m2msupport.net/m2msupport/module-tester/. [Accessed 02 April 2015].

[13] FlexiSPY, “Spy on Mobile Phones, Cellphones & Tablets,” FlexiSPY, 2015. [Online]. Available: http://www.flexispy.com/. [Accessed 02 April 2015].

[14] D. G. Raptodimos, Design and implementation of an Android application for extraction of security related data from SIM/USIM, Piraeus: University of Piraeus, 2013.

[15] S. Malliaros, “SSL-Unipi / U-SIMonitor,” 28 February 2015. [Online]. Available: https://github.com/SSL-Unipi/U-SIMonitor. [Accessed 02 April 2015].

[16] ETSI, “Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 9),” ETSI, 2010.

[17] Google, “Android Platform Development Kit v.03,” netmine.com, June 2008. [Online]. Available: http://www.netmite.com/android/mydroid/development/pdk/docs/telephony.html. [Accessed 02 April 2015].

[18] R. Fedler, J. Schütte and M. Kulicke, “On the effectiveness of malware protection on Android,” Fraunhofer AISEC, 2013.

[19] 3GPP, “3GPP TS 27.007 V11.5.0 (2012-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; AT command set for User Equipment (UE) (Release 11),” 3GPP, 2012.

[20] 3GPP, “3GPP TS 35.201, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification (Release 9),” 3GPP, 2009.

[21] 3GPP, “3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9),” 3GPP, 2009.

[22] K. Nohl, “Attacking phone privacy,” in *Black Hat USA 2010*, Las Vegas, Nevada, 2010.

[23] A. Orozco, “Mobile advertisers use malware tricks to get installs,” Malwarebytes Unpacked, 10 October 2014. [Online]. Available: https://blog.malwarebytes.org/mobile-2/2014/10/mobile-advertisers-use-malware-tricks-to-get-installs/. [Accessed 02 April 2015].

[24] A. Ruiz, “apk_binder_script,” funsecurity.net, 07 April 2014. [Online]. Available: https://github.com/funsecurity/apk_binder_script. [Accessed 02 April 2015].

[25] V. Rastogi, Y. Chen and X. Jiang, “Droidchameleon: evaluating android anti-malware against transformation attacks,” in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIACCS 2013)*, Hangzhou, China, May 2013.

[26] OneClickRoot, “Need Help Rooting Android?,” OneClickRoot, 2015. [Online]. Available: http://www.oneclickroot.com/. [Accessed 02 April 2015].

[27] I. Androulidakis, D. Pylarinos and G. Kandus, “Ciphering Indicator approaches and user awareness,” *Maejo International Journal of Science and Technology*, vol. 6, no. 3, pp. 514-527, 2012.

BIOGRAPHIES

Editors and Co-Editors

Bernhards Blumbergs is a researcher at NATO CCD COE Technology branch. He is a certified exploit researcher and advanced penetration tester (GXPN), and a team member of the Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV). He has a strong military background, targeted at developing, administering and securing wide area information systems. He is also a Cyber Security PhD student at Tallinn Technical University, with his research focusing on methods for network security mechanism evasions.

Cpt **Pascal Brangetto** is a supply officer in the French Army. He graduated from the Military Administration Academy in 2006 and served as a 1st lieutenant at the 4th French Foreign Legion Batallion as a deputy administrative and supply officer. Then he went on to serve as an administrative and supply officer at the 1st Medical Battalion in Metz and was deployed for a tour of duty in Afghanistan during the ISAF operation in 2010. Before being posted as a legal researcher at NATO CCD COE in 2013, he was a staff officer in the French Joint Supply Service Directorate in Paris. Captain Brangetto is a graduate from the Institut d'Etudes Politiques in Aix-en-Provence.

Dr **Lauri Lindström** is a researcher at NATO CCD COE since May 2013. Prior to joining NATO CCD COE he worked at the Estonian Ministry of Foreign Affairs (2007-2012) as the Director General of Policy Planning and held various positions at the Ministry of Defence (1995-2007) dealing mainly with issues related to international cooperation, Estonia's accession to NATO, defence planning and security policy. Lauri Lindström holds a Ph.D. from the Tallinn University, Estonia.

Cpt **Markus Maybaum** is a German Air Force officer with more than 20 years of professional experience in the field of IT and IT security. Before his current assignment as a researcher at NATO CCD COE's Research and Development Technology Branch, he worked in several different national and international management, leadership and expert positions focussing on information technology, software engineering, cyber security and arms control. Besides a diploma in business administration from the German Air Force College, Markus holds a Master's Degree in informatics from the German Open University of Hagen specializing in IT security and he is currently pursuing a PhD in information technology with a focus on technical aspects of arms control in cyber space at Fraunhofer FKIE, Germany. Markus lives in Estonia together with his wife Simone and their four children.

Anna-Maria Osula is a researcher at NATO CCD COE Law & Policy branch. During her time with the Centre she has been involved with projects like CyCon, Cyber Coalition, Locked Shields, and published research on different aspects related to national cyber security strategies, international organisations and cyber defence. She is also a lecturer at the Tallinn Technical University Cyber Defence Master Programme, and a frequent presenter at international conferences. Anna-Maria holds an LLM degree in IT Law from Stockholm University and is working towards a law PhD at Tartu University, Estonia.

Maj **Nikolaos Pissanidis** is a Greek Army IT officer with more than 20 years of professional experience in the field of IT and IT security. Before his current assignment as a researcher at NATO CCD COE's Research and Development Technology Branch, he worked in several different national and international management, leadership and expert positions focussing on information technology, software development, cyber security and penetration testing. Besides a diploma from the Hellenic Army Academy, Niko holds a master's degree in New Technologies in Informatics and Telecommunications from the Department of Informatics and Telecommunications of National and Kapodistrian University of Athens.

Henry Rõigas works for NATO CCD COE's Law and Policy branch since 2014. His research areas in the Centre include policy-related matters such as state interests in global cyber affairs, the role of international organisations and small states in cyber security and cyber defence cooperation within NATO. He holds a master's degree in International Relations from the University of Tartu.

Matthijs Veenendaal has been working for the Netherlands Ministry of Defence since 2006 in various policy positions. He is currently stationed as a researcher at the Strategy Branch of the NATO CCD COE in Estonia. He has been closely involved in the development of cyber defence policy of the Ministry of Defence and the principle author of the first Defence Strategy for operating in cyberspace (2012). He was also closely involved in the development of the two National Cyber Security Strategies of the Netherlands. Matthijs studied contemporary history at the university of Leiden and political science at the University of Texas, Austin.

Teemu Uolevi Väisänen is currently working as a researcher for NATO CCD COE. He is studying for Ph.D. at the University of Oulu and works for the Finnish Defence Forces as Researcher. Mr.Väisänen was working for VTT Technical Research Centre of Finland (VTT) as a Research Trainee (2005-2006), graduated with an M.Sc. in Technology degree in Information Engineering, Embedded Systems, the University of Oulu (2006), and started his appointment as a Research Scientist at VTT, Oulu, Finland in October 2006. His work consists of different topics of information and cyber security. He has been working in international and national projects in which he has worked mostly with security of Smart Grids, Internet of Things, wireless mobile ad-hoc routing protocols, Machine-to-Machine, and smart phones. Väisänen worked as a voluntary Safety Expert of VTT, in Safer Internet Day (SID) project led by Finnish Communications Regulatory Authority (2006-2012) and since 2013 as one of VTT's voluntary Mediataitokummi in Media Literature School project led by the National Audiovisual Institute (Finland). His current research interests include cyber security, Internet of Things and privacy.

Authors

Sergei Boeke joined the Leiden University Campus The Hague as a fellow in February 2013. After completing Officer training for the Royal Netherlands Navy, he studied law at the Vrije Universiteit Amsterdam, specializing in international and criminal law. He held several posts in the Navy, serving on different warships and with the Second Marine Battalion on operations abroad. After a short posting as fellow at the Netherlands Institute for International Relations Clingendael, he joined the diplomatic service and worked for the Department of Political Affairs in The Hague. Moving back to the Ministry of Defence in 2008, he was involved in supporting the Dutch comprehensive approach mission in Afghanistan. In 2011, he completed a nine-month course for civil servants at the Ecole Nationale d'Administration (ENA) in Strasbourg, France. His current research focuses on cyber security governance issues, and he lectures at the Cyber Security Academy in The Hague.

Robert Brose currently serves as the ODNI Lead for Futures and Capability Development. In this position, he leads Intelligence Community (IC) forecasts of the emerging global Scientific and Technological (S&T) environment, facilitates IC leverage of worldwide R&D activities, and champion's strategies and proof-of-concept demonstrations that realign and strengthen the relationship between IC analysis, research and development, and planning. In prior roles, he directed a multi-million dollar laboratory-to-field technology portfolio as manager of the IC's Rapid Technology Transition Initiative, and held both technology-focused and regionally focused analytic positions within the Department of Defence. There, as a Sino-Southeast Asia issues expert, he participated in the 2011 bilateral defence and defence policy dialogues with the Socialist Republic of Vietnam, and as Chair of the S&T Surprise Working Group, represented DoD abroad to expand partnerships with allies. Mr. Brose has been invited to speak on technology and international relations issues in a variety of settings, ranging from industry events and the Phoenix Challenge conference series, to classes at the NATO school, in support of studies at the National Academy of Sciences, and at Zhongshan University in Guangzhou, China.

Matteo Casenove graduated at the Amsterdam Vrije Universiteit in MSc Parallel and Distributed Computer Systems. He is a contractor with the NATO CCD COE for teaching a course in Botnet Mitigation. He worked as intern at NATO CCD COE on Malware Analysis and Active Cyber Defence. Moreover, he worked as research assistant at Kent University in UK in Federated Access for Cloud. He has a strong passion and interest in everything related to Cyber Defence and Cyber Warfare.

Maj **Geoffrey S. DeWeese** works in the United States Army's Judge Advocate General's Corps. His most recent assignment was as Chief, Cyberspace Operational Law and Deputy Chief, International and Operational Law, U.S. Strategic Command. He is a graduate of Seattle Pacific University with a BA in History (1994), University of Denver College of Law with a JD (1999), and The Army Judge Advocate General's School with an LLM in Military Law (2008). Originally from the state of Colorado, Geoff has served in numerous assignments around the world in both military justice and operational law and has prior service as an enlisted member of the Army Reserves.

Mario Golling is a PhD student at the Universität der Bundeswehr München (UniBwM), where he graduated in business informatics in 2007. His key aspects of research activity are network security, cyber defence, intrusion detection and next generation internet. He has many years of experience in running operational networks as well as teaching and training network administration/security. Among other things, he is a member of the Working Group IT Security of the UniBwM.

Dr **Richard Hill** has an extensive background in information systems, telecommunications, negotiation, mediation, and conflict management. He was the Secretary for the ITU-T Study Groups dealing with numbering and tariffing issues, network operations, and economic and policy issues; he was the Secretary for the preparatory process for the 2012 World Conference on International Telecommunications and headed the secretariat team dealing with substantive issues at the Conference. He has facilitated numerous complex international negotiations regarding sensitive policy matters, including Internet governance.

Margarita Jaitner is currently a researcher within the Russia Project at the Swedish Defence University, focusing on Russian Information Warfare and the use of Cyber for Information Operations. She graduated from the SDU with a BA degree in Political Science and from Karlstad University with an MA degree in Societal Risk Management. In the past she has worked at the Finnish National Defence University and the Yuval Ne'eman Workshop for Technology, Science and Security at Tel Aviv University.

Alexis Le Compte is a PhD student at De Montfort University, Leicester, England. He also holds an MSc in Computer Security and BSc in Computer Science. His research focuses on applications of serious games for cyber security. He is developing a flexible framework for the design of serious games, to raise awareness of cyber security principles to audiences with limited knowledge of cyber.

Dr **Mirco Marchetti** is a researcher of the Inter-department Research Center on Security (CRIS) at the University of Modena and Reggio Emilia, Italy. He received the Laurea degree and the PhD in Computer Engineering from the University of Modena with projects on large scale systems for information security. He is an expert in cooperative network intrusion detection and prevention, fault tolerant distributed systems, high performance systems for information security management and cloud security. He is a teacher in the Master in Cyber Defence organized by the Armed Forces Institute of Telecommunications and the University of Modena and Reggio Emilia.

Tim Maurer is the Director of the Global Cybersecurity Norms and Resilience Project and Head of Research of New America's Cybersecurity Initiative. He is part of New America's Future of War project and serves as a member of the Research Advisory Network of the Global Commission on Internet Governance, the Freedom Online Coalition's cybersecurity working group "An Internet Free and Secure", and co-chair of the Civil Society Advisory Board for the Global Conference on Cyberspace. His current research focuses on cyberwarfare and the global cyber-security norms process as well as transatlantic cooperation on security and freedom in the digital age. Previous projects have also focused on Internet Freedom, especially in the context of U.S. sanctions and export controls, and research on swing states in the international Internet governance debate. In 2013 and 2014, Mr. Maurer spoke about cyber-security at the United Nations in New York and Geneva in addition to other national and international conferences. His research has been published by Harvard University, Foreign Policy, CNN, TIME, Jane's Intelligence Review and Slate among others. Prior to joining New America, Mr. Maurer worked at the Center for Strategic and International Studies and gained experience with the United Nations in Rwanda, Geneva, and New York focusing on humanitarian assistance and the coordination of the UN system. He holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School.

Uchenna Jerome Orji is an Attorney admitted to the Nigerian Bar as a Barrister and Solicitor of the Supreme Court of Nigeria. He holds an LL.B Honours Degree from the University of Nigeria and, an LL.M Degree with distinctions from the University of Ibadan, Nigeria, where a major part his research focused on Information Technology Law and cybersecurity governance. He is currently completing a PhD in law at the Nnamdi Azikiwe University in Nigeria, with a specialization in telecommunications regulation. Uchenna is also a Research Associate at the African Center for Cyber Law and Cybercrime Prevention (ACCP) located within the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders in Kampala, Uganda. He is the author of Cybersecurity Law and Regulation (Wolf Legal Publishers: The Netherlands, 2012), in addition to several journal publications on cybersecurity law and also works as a consultant for a number of local and international organizations.

Jason Rivera is a professionally published and certified cyber, intelligence community, and military operations expert who possesses over eight years of experience innovating at the intersection of defence operations and technology. He is currently employed in Deloitte's Threat Intelligence & Analytics practice where he specializes in the build out of cyber intelligence and cyber operations programs for both federal and commercial clients. Prior to Deloitte, Jason served over six and a half years in the military as an Intelligence Officer where he attained the rank of Captain and served in various positions to include roles at the National Security Agency (NSA), United States Cyber Command (USCYBERCOM), and other cyber elements. In additional to his professional achievements, Jason is an established academic writer to include work published at the NATO Cooperative Cyber Defence Centre of Excellence, Small Wars Journal, and several other scholarly publishing forums.

Alison Lawlor Russell is an assistant professor of Political Science and International Studies at Merrimack College and a non-resident research scientist at the Center for Naval Analyses. Dr. Russell is author of the book Cyber Blockades (Georgetown University Press, 2014) and a forthcoming chapter on the implications of cyberspace in the Routledge Handbook of Naval Strategy and Security (September 2015). She holds a PhD from the Fletcher School of Law and Diplomacy at Tufts University, an M.A. in International Relations from American University in Washington, D.C., and a B.A. in Political Science from Boston College.

Dr **Jennifer Stoll** is a Visiting Researcher at the Technical University of Munich with the Chair for Philosophy of Science and Technology. The focus of her work is on developing novel visualization approaches for supporting public policy.

Paul A. Walker is Counsel to the Commander, Fleet Cyber Command/10th Fleet, where he practices the cyber aspects of contracts, fiscal, business and intelligence law. Paul previously served in cyber and intelligence law billets with the Navy Office of the Judge Advocate General; U.S. Cyber Command; DoD General Counsel; and Office of Naval Intelligence. Paul teaches Cyber Threats and Security at American University, military law at the U.S. Naval Academy and cyberlaw at National Defense University. Paul graduated from the U.S. Naval Academy, has a Masters in International Studies from Old Dominion University, his Juris Doctor from William & Mary Law School; and his Master of Laws degree in National Security and U.S. Foreign Relations Law from the George Washington University. Prior to attending law school, Paul was a U.S. Navy pilot and intelligence officer.

Dr **Christos Xenakis** received his B.Sc degree in computer science in 1993 and his M.Sc degree in telecommunication and computer networks in 1996, both from the Department of Informatics and Telecommunications, University of Athens, Greece. In 2004 he received his Ph.D. from the University of Athens (Department of Informatics and Telecommunications). From 1998 – 2001 he was with a Greek telecoms system development firm, where he was involved in the design and development of advanced telecommunications subsystems. From 1996 – 2007 he was a member of the Communication Networks Laboratory of the University of Athens. Since 2007 he is a faculty member of the Department of Digital Systems of the University of Piraeus, Greece, where currently is an Assistant Professor and member of the System Security Laboratory. He has participated in numerous projects realized in the context of EU Programs (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie) as well as National Programs (Greek) and his research interests are in the field of systems, networks and applications security.