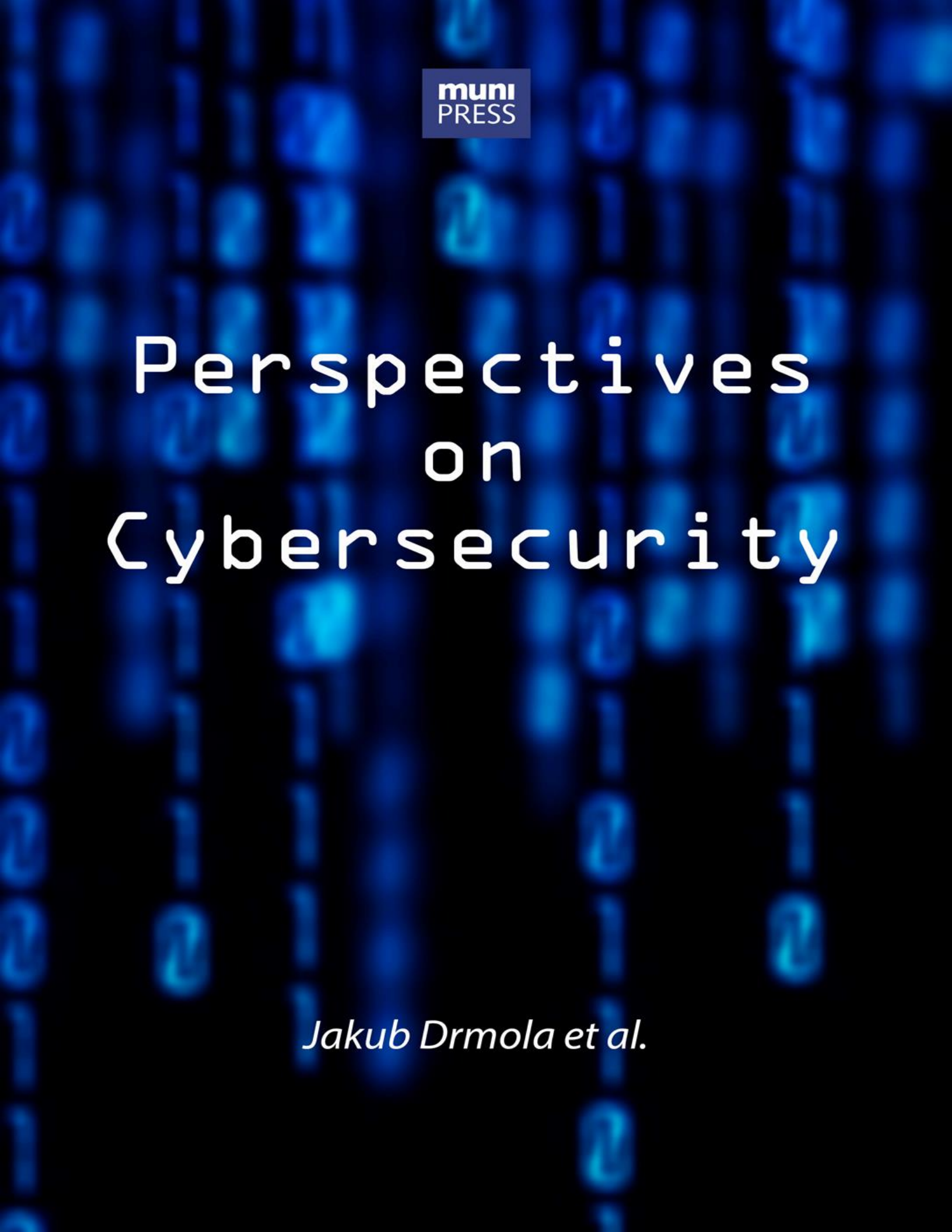
muni
PRESS
Perspectives
on
Cybersecurity
Jakub Drmola et al.

Masaryk University

Perspectives on Cybersecurity

Jakub Drmola et al.

Brno 2015

Global Politics
www.globalpolitics.cz/en

The publication was developed by Global Politics journal and published by the Masaryk University.

Global Politics is associated with the International Institute of Political Science and the Department of International Relations and European Studies of Masaryk University, Brno. It publishes scholarly texts from International Relations and related disciplines.

Pre-publishing review: Mgr. Roman Pačka

ISBN 978-80-210-7870-3 (online : pdf)

Foreword

This book comes at a time of utmost interest in cybersecurity. Our incessantly growing dependence on information and communication technologies, the seemingly unstoppable proliferation of computers into all aspects of modern life and the very ubiquity of digital media come hand in hand with increased concerns for our security. Unfortunately, this increased interest often seems to be ahead of research and scholarly debate. Furthermore, the overlap between technical and social aspects of cybersecurity has proven difficult to understand and untangle. The regrettable result is that misconceptions, exaggerations and distortions are rife in the media, politics and public debates. The purpose of this publication then is, among others, to inform the debate, to facilitate research and to provide insights into this complicated domain in order fight discrepancies between social perceptions and social reality.

This particular publication brings together expertise from a wide range of scholars from various universities and faculties. Each brings his or her own approach to the research of this field. Individual chapters can be regarded as semi-independent case studies with their own merits and limitations. But crucially, they also create a more comprehensive image of cybersecurity when put together into a greater whole. Furthermore, this scope and structure make it possible to assess which methods of analysis might be most appropriate for future research of different topics.

This book essentially represents a snapshot of the general state of cybersecurity captured by the authors during the year 2014. We start by exploring the most pressing aspects of conflict in cyberspace: the feasibility of a full-blown cyberwar, principle of distinction during such a conflict, and issues of deterrence. Possibly even more practical side of cybersecurity is then elucidated in the two following chapters detailing the recent deluge of APTs and concerns about the Chinese telecom giant. The next chapter introduces the crucial matter of international cooperation in the field of cybersecurity. The subsequent chapter about the issues of human rights and Internet freedoms in Russian Federation seems to be dealing with a chronic problem which is current in 2015 as it was in 2014. And finally, we close with a study of the concept of cyberspace security itself, while the very last chapter applies it to the familiar and ever-controversial issue of Internet piracy.

This wide range is not only indicative of newness of the discipline but it also directly reflects the multitude facets of cybersecurity and the breadth of its impact on our society. Topics covered in individual chapters are as varied as human rights, law, wars, media, international order, economy, and espionage. Naturally, all of these areas have very strong links to cybersecurity.

While the chapters cover many different topics, this publication by no means covers the entire scope of cybersecurity. In some ways, it just scratches the surfaces and leaves many problematic areas mostly untouched. Nevertheless, it is sorely needed and more work will be necessary before our society fully comes to grips with cyberspace and all it entails.

Table of Contents

Table of Figures

Abbreviations

ACTA - Anti-Counterfeiting Trade Agreement
APEC - Asia-Pacific Economic Cooperation
APT - Advanced Persistent Threat
ASEAN - Association of Southeast Asian Nations
BAE - British Aerospace Systems
BGP - Border Gateway Protocol
C2, C&C – Command and Control
C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCD COE - Cooperative Cyber Defence Centre of Excellence
CCW - Changing Character of War
CERT – Computer Emergency Response Team
CNE - Computer Network Exploitation
CNO - Computer Network Operations
CPNI - Centre for the Protection of National Infrastructure
CoE - Council of Europe
DCS - Distributed Control Systems
DDoS– Distributed Denial of Service
DIB - Defense Industrial Base
DNS – Domain Name System
DoD – Department of Defense
FSB - Federal Security Service of the Russian
GAO – Government Accountability Office
GPS – Global Positioning System
HWP - Hangul Word Processor
ICJ - International Court of Justice
ICT - Information and Communication Technology
IETF - Internet Engineering Task Force
IFPI - International Federation of the Phonographic Industry
IHL - International Humanitarian Law
IO - Information Operation
IP – Internet Protocol
ISP – Internet Service Provider
ITU - International Telecommunication Union
LTE - Long Term Evolution
MLAT - Mutual Legal Assistance Treaty
MoD – Ministry of Defense
NISCC - National Infrastructure Security Co-ordination Centre
NSA – National Security Agency
OECD - Organization for Economic Co-operation and Development
OSCE - Organization for Security and Co-operation in Europe
PIPA – Protect Intellectual Property Act
RAND - Research And Development
RAT – Remote Access Tool
RIA - Russian Information Agency
RMA - Revolution in Military Affairs
RSA - Rivest, Shamir, Adleman
SCADA - Supervisory Control and Data Acquisition
SCO - Shanghai Cooperation Organization
SOPA - Stop Online Piracy Act
SSRC - Social Science Research Council
URL - Uniform Resource Locator
VPN – Virtual Private Network
WMD – Weapon of Mass Destruction
WTO – World Trade Organization

Summary

The book you are about to read provides a broad look into the realm of cybersecurity. Topics covered in individual chapters are as varied as they are current. Despite the immediacy of these issues and threats, the general understanding of cybersecurity among the public, the media, and the policymakers is still severely lacking. Following pages can therefore be helpful and interesting to concerned laypeople as well as to scholars and practitioners.

The first four chapters are focused on the aspects of conflict in cyberspace. These are mainly the issues of attribution, distinction, proportionality, and deterrence, which are both crucial and fairly controversial. This is problematic on all levels – social, strategic, as well as legal one. The overall picture painted by the authors is quite bleak. But this bleakness lies in our profound lack of comprehension and adaptation to this new cyber-infused world and not in our immediate doom. In other words, it is still exceedingly difficult for us to tell who is doing what in cyberspace, find appropriate responses to various attacks, or even to protect ourselves from such attacks. The seemingly never-ending string of APT intrusions makes this difficulty painfully apparent. Furthermore, operations in cyberspace are becoming a natural part of any conflict in the physical world. All the shots being fired on the contemporary battlefields carry their echoes deep into cyberspace and we need to figure out how to react to this new reality.

The fifth chapter further illustrates some of these difficulties on the example of Huawei, which blends the lines between economy, politics and security. It is a manifestation of the troubling lack of distinction between civilian and military domains in cyberspace.

The remaining chapters are more varied and mostly deal with the institutional and international aspects of cybersecurity. Multilateral cooperation, regulations and overarching frameworks play increasingly important role, but, yet again, clear cut answers and solutions are hard to come by and even harder to agree upon. Countries adopt different sets of laws in an effort to control and govern their cyberspace, but it remains unclear what "their" cyberspace even is, despite so many countries trying to claim some sort of sovereignty over it. Further still, overly contrasting norms lead to clashes over the appropriate levels of freedom and security, which is best demonstrated on the example of Russian Federation. Problems in this area are further compounded by the ongoing conceptual and social reconstruction of cybersecurity itself.

Tomáš Maďar

Introduction

The emergence and spread of information and communication technologies (ICT) at the advent of the third millennium has undoubtedly caused a revolution in the way information and knowledge are being stored and shared. The information revolution is sometimes ranked as high as second in its impact, topped only by Gutenberg's invention of the printing press.

In the new era we live in – the information age – many of the physical barriers have disappeared: connecting and communicating with someone on the other side of the world, sharing information and knowledge, learning about a variety of topics, even visiting places and downloading multimedia, gaining access to previously unimaginable resources – this and much more has been made available thanks to the emergence of ICT and the global interlinked network, the Internet.

The highly interconnected world causes massive implications for communication, business, education and learning, in essence our everyday life. We are increasingly growing accustomed and often even reliant on, our information structure and functioning networks. As ICT spreads into almost all spheres of human activities, they grow more and more connected to each other, including critical national infrastructure as well as other critical.

The aforementioned fact is understandable, since being able to easily operate our systems and networks with ICT allows us to maintain and manage our critical infrastructure more efficiently. This, however, comes at a price – these systems, while protected to a certain point, remain rather vulnerable to an attack. The immense linkage between the systems and networks, the reliance on the functioning of ICT and the fact that the nation states need their critical infrastructure to be functional in order to fulfil their various tasks and roles means that with the increased utilization of the Internet and other networks, new threats and risks have emerged.

In recent years, these threats have been articulated – cybercrime has taken a hold, although some speculate that it barely exploited new technologies to transfer traditional crimes into the domain of cyberspace; in 2004, the first convention on cybercrime entered into force (Council of Europe 2013). There have also been numerous instances of politically motivated hacking and cases of what has been called "hacktivism" – the utilization of cyberattacks by activists with the intention to reach political goals.

An entirely different ballgame would then be cyber espionage. Theft of intellectual property and related crimes, as well as the infiltration of a variety of key networks and systems that store and transmit sensitive information has reached levels previously unimaginable. Apart from massive economic losses caused especially to businesses and countries of the post-modern western world due to technologies and other data being stolen, cyber espionage now plays a vitally important role in the (in)security of nations. To say espionage has caused a shift in the balance of power would be an exaggeration; however, some of the incidents, such as the plans of a new generation of fighter jets being stolen or the leaks of diplomatic cables, not to mention the recent NSA affair, might prove significant in the long run.

The information revolution has even touched the way contemporary conflicts are being fought – the omnipresence of information and communication technology means these are also utilized by most modern militaries – many armed forces use ICT for a wide spectrum of capabilities. These technologies have proven themselves as a significant force multiplier when used both on and outside of the battlefield.

The potential of the cyber component has led some to believe that cyberspace might be a domain of a type of new (cyber) warfare that could even be led separately, without resorting to the traditional form of warfare. In the last decade, numerous attempts to conceptualize cyber warfare (or even cyberwar, for that matter) as well as estimate its strengths, weaknesses and limits have been made, much to little avail. The consensus has not yet been reached and while there might be certain potential, it remains a matter of dispute.

While there have already been some attempts to regulate this new form of warfare due to the insufficiency of current legislation, this endeavour is yet in its infancy. Even the most accomplished attempt so far, the Tallinn Manual, (Schmitt et al. 2013) is still but a draft, and its eventual success or failure concerning the future shaping of cyber warfare regulation is yet to be determined.

Aims and Methodology

This chapter aims to introduce the sceptical approach towards the idea of a potential cyberwar taking place in the near future. In order to do so, a reflection of the current approaches to cyber warfare must be made and therefore several concepts of cyber warfare and cyberwar need to be presented and reflected upon. This entails not only a set of definitions, but also a critique of the very notion of cyberwar – in recent years, the emerging sceptic voices have sometimes even rejected the very idea that a cyberwar might be a possibility, not to mention a likely one.

During the process of working on the chapter, we utilize the method of hermeneutics to process secondary literature concerning the topic of cyber conflict, cyber warfare and cyber war. Thanks to observations made this way we will then try to explain and reflect upon the sceptical approach to the aforementioned topic.

The aim of the chapter is to describe the very origins of the concept of cyberwar and to sum up some of the often-stressed arguments as to why cyberwar is unlikely to happen in the near future, since these arguments offer a valuable critical approach to the heated debate within the security community. To conclude, the critical standpoint accentuating the lower likelihood of a cyberwar taking place in the present and/or the near future is explained.

Existing Concepts, Clashing Attitudes

The First Concepts of Cyberwar

According to Geers, a forthcoming „information war“ in cyberspace was allegedly first mentioned by Thomas Rona, the author of a 1976 Boeing Corporation research paper „Weapons Systems and Information War“. Rona argued that should a war break out, computer systems would be among the first targets of military campaigns. Based on his claims, “all information flows within any command-and-control system are vulnerable to jamming, overloading, or spoofing by an adversary.” (Geers 2011)

The potential of the Information Revolution concerning information warfare was then further elaborated by a widely cited 1993 article by Arquilla and Ronfeldt, which also examined some of the historical aspects of what the authors labelled “cyberwar”. Aptly named “Cyberwar Is Coming!” the concepts developed in the article were in many respects revolutionary and well ahead of their time. Arquilla and Ronfeldt envisioned two distinct levels of conflict involving cyberspace:

1. A netwar, which is closely tied to soft power and propaganda; the authors claim “most netwars will be non-violent, but in the worst of cases one could combine the possibilities into some means of low-intensity conflict scenarios.”
2. A cyberwar, which mostly encompasses the military utilization of cyberattacks designed to disrupt, if not destroy, the adversary’s information and communication systems (the definition was then made broad enough to incorporate the military culture of the adversary). Arquilla and Ronfeldt state “cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design. It may be applicable in low- and high-intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes” (Arquilla and Ronfeldt 1993).

The authors also link the emergence of cyberwar to the Revolution in Military Affairs – their article anticipates that the concept of cyberwar might be to the 21st century what blitzkrieg was to the 20th century. On the other hand, they flat-out refused to precisely define the concept due to it being rather speculative at the time. Moreover, several concepts or historical applications of strategies closely tied to (or preceding) the concept of cyberwar were closely examined – such as those of ancient Carthaginians, medieval Mongols, the British Royal Navy in the late 18th century, or the Third Reich’s concept of

blitzkrieg during the Second World War. The authors also described two of the probably most defining conflicts of the second half of the 20th century (at least from the American perspective): the Vietnam War and the First Gulf War, as well as the implications these conflicts bear for the concept of cyber warfare.

In 2001, Timothy Shimeal, Phil Williams and Casey Dunlevy wrote an article for the NATO Review, inside of which the three argue that defence planning should incorporate the virtual world in order to limit the amount of physical damage that can be done by cyberattacks "in the real" (sic!) one. The authors deny the vision of a conflict in which cyberwar would be a phenomenon completely isolated from broader conflict – they claim that the scenario of cyberwar operating in an altogether different realm from traditional warfare and offering a bloodless alternative to its costs and dangers may not be "beyond the realm of possibility", but is nonetheless rather unlikely.

Shimeal, Williams and Dunlevy stress that advanced post-industrial societies and economies depend critically on information and communication systems that are interlinked. Also, cyber components have become an increasingly important part of contemporary military capabilities, up to a point where they are considered to be major force multipliers (or, in contrast, equalisers). This, however, leads to a certain dependence on such technologies – such dependence can then become a vulnerability of the entire military establishment; a proverbial "Achilles' heel." According to the aforementioned authors, such a potential is not limited to military infrastructure – "[d]isruption of civilian infrastructures is an attractive option for countries and non-state actors that want to engage in asymmetric warfare and lack the capacity to compete on traditional battlefield" (Shimeal, Williams and Dunlevy 2001).

The trio distinguishes between three levels of cyberwar:

1. Cyberwar as an adjunct to military operations
2. Limited cyberwar
3. Unrestricted cyberwar

The first category revolves around how contemporary battles are being fought – modern military establishments involved in hostilities aim to achieve information superiority (or dominance) in the battle space. This can be achieved by ensuring a precise oversight of the battlefield, as well as preventing the adversary from gaining such an oversight by attacking his systems and actively taking steps in order to increase the enemy's fog of war (while doing the utmost to reduce it for one's own forces).

The limited cyberwar usually targets the enemy's networks and is usually accompanied by little to no real-world (sic!) action. The targeted infrastructure should form "a means by which the effectiveness of the enemy is reduced". Thus, limited cyberwar aims to slow the enemy down, constraint an adversary's manoeuvrability during a crisis or to induce economic damage.

The third category, allegedly both more serious and more likely, is what the authors termed an unrestricted cyberwar. Three major characteristics are listed to this form of warfare: first, it would be comprehensive in scope and would make no distinction between military and civilian targets, between home front and fighting front. Second, it would have physical consequences and casualties. Third, the economic and social impact could be profound. The prime targets in such a campaign would probably consist of critical infrastructure facilities (ibid.).

Shimeal, Williams and Dunlevy therefore (albeit vaguely) define some of the elementary characteristics of cyberwar, and present an idea of what such a form of modern warfare might look like. Apart from the perceived targets and possible effects of a hypothetical cyber campaign, the most notable points of the article are the depictions of what the authors deem respective categories of cyberwar – especially of the limited one, which seemingly does not require casualties in order to be considered a cyberwar.

The Alarmists and the Sceptics: Where Does the Truth Lie?

In a 2009 Conference on Cyber Warfare contribution, Martin Libicki (2009) analysed the prospect of sub rosa warfare in cyberspace. Libicki defines cyber war "as consisting of computer network (more broadly, systems) attack and defence. An attack succeeds when the target's use of his own systems is hampered – either because such systems fail to work or work very efficiently (disruption) or because systems work but produce errors or artefacts (corruption)." Libicki specifically excludes Computer

Network Exploitation (CNE – "cyber espionage"), which he considers a different phenomenon: „Spying is not an act of war. It never has been, and there's little reason to change that"". This is an interesting approach, since Computer Network Exploitation is often categorized as part of the computer network operations[1] (CNOs). It should also be noted that in this rather specific study, Libicki focuses solely on state-on-state cyber warfare.

Libicki is otherwise rather sceptical about the notion that a cyberwar might take place – he states that the perception of the risk of a debilitating cyberattack, albeit real, is far greater than the actual risk. Although the Internet has been around for a while and it has been used for offenses many times already, "no person has ever died from a cyberattack, and only one alleged cyberattack has ever crippled a piece of critical infrastructure, causing a series of local power outages in Brazil." (Libicki 2013)

In recent years, the very notion of cyberwar has been widely and thoroughly discussed – and to say the discussion was polarized would definitely be an understatement. Quite a few authors from different backgrounds including academia, governments and authorities, as well as computer security have shared their views concerning the likelihood and possible effects of a cyberwar occurring.

It seems two polarized "camps" with rather distant opinions have been the most vocal when discussing the issue – the pessimistic voices are sometimes labelled as the alarmists while those challenging or rejecting the idea of a cyberwar happening (or having any decisive impact at all, for that matter) are often called cyber sceptics. The Cato Institute lists a vast number of articles and papers, the authors of which believe the threat from cyberattacks has recently been greatly exaggerated (Mueller and Friedman 2014).

Mueller and Friedman consider much of the recent debate about cybercrime, cyberterrorism and cyberwar in the United State to be "alarmist in the extreme" – as a major example the book "Cyberwar: The Next Threat to National Security and What to Do About It" by Richard Clarke and Robert K. Knake, a 2010 bestseller, is often criticized. In the book, the authors not only describe contemporary cyber issues and demonstrate them on recent incidents (such as the Israeli aerial strike on the supposed Syrian nuclear reactor to be enabled by a cyberattack on the Syrian anti-aircraft defences, or the attacks on the Estonian ICT systems in 2007), but also present what a cyberwar in its extreme case could look like, which seems to be a major source of their work's subsequent criticism[2] (Clarke and Knake 2010).

Clarke and Knake define cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption". According to them, such actions are on the rise. The two authors also claim that the more connected a nation is, the more vulnerable it becomes – therefore, advanced nations and powers, such as the United States or Estonia, would have much to lose should a cyberwar break out (ibid).

Many of those who are often criticized as alarmists by the sceptics recruit themselves from intelligence agencies, government agencies, security branches of the state apparatus or various branches of respective states' armed forces. There is a plethora of ways how to demonstrate that in the recent years cyber threats are being addressed more than ever, sometimes even ad absurdum – for instance, in 2009 a top US commander, General Kevin Chilton, even proclaimed that the United States should retain the option to respond (to cyberattacks) with physical force – potentially even using nuclear weapons (Grossman 2009). The Defense Secretary of the United States, Leon Panetta, warned in October 2012 that the country is facing a possibility of a "cyber-Pearl Harbor"[3] (Bumiller and Shanker 2012). More accounts can be provided by Lynn (2010) or the aforementioned Shimeal, Williams and Dunlevy (2001).

[1] These are operations usually closely linked to cyber warfare – for instance, the United States' National Security Agency's definition of CNOs involves three major functions: Computer Network Attack, Computer Network Defense, and Computer Network Exploitation (National Security Agency 2013). Probing of computer systems and networks, often a precursor for the subsequent attack, is hard to distinguish from espionage.

[2] See Harper 2010, Schneier 2010, Singel 2010.

[3] Rid disagrees with the notion of a cyber-Pearl Harbor (Rid 2011). Mueller (1991) explains, how this incident may have been a political disaster and a significant historic moment, but from the military standpoint, hardly a nuisance.

The US intelligence community under the auspices of the director of national intelligence, James D. Clapper, also issued a 2013 assessment of global threats to the United States of America – cyber threats were ranked at the very top, followed by terrorism, transnational organized crime, proliferation of WMDs, etc. (US DoD 2013a).

But the United States are not the only nation state that has recently delved into cyber security research – the United Kingdom is working on a plan to limit cybercrime and bolster the country's offensive capabilities (Elwell 2013). India and Pakistan have already experienced a lot of offensive cyber activity from hackers on both sides – India has recently even called its patriotic hackers to arms (Times of India 2010).

The worst alleged perpetrators (at least from the Western perspective) of offensive cyber activities – China (see Ball 2011) and Russia (see Heickerö 2010) (with Iran on the rise after the infamous Stuxnet affair[4]) – are also investing into the development of cyber capabilities. And so is Israel (see Defensetech 2010) as well as other countries.

A Rejected Notion

Lately, there have been discussions about whether or not offensive campaigns in cyberspace might substitute traditional forms of political violence and even interstate conflict. However, when it comes to the very notion of cyberwar, there are quite a few experts who challenge the idea, reject it, or outright denounce it. One of them is Thomas Rid.

In his article (and later book), aptly named "Cyberwar Will Not Take Place", Rid criticizes what he calls the "Cassandras of cyber warfare" – the members of establishment hyping the potential of cyber threats in recent years. Rid argues that a cyberwar has not happened yet, was not happening at the time of writing the article, and is unlikely to ever happen. All of the cyberattacks that have been witnessed up to this point have then been "merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage." Rid then questions the probability of this being changed in the future.

The main reason Rid disqualifies offensive cyberattacks as potential acts of war is that until today there are no proven recordings of a lethal cyberattack ever taking place. The author quotes Clausewitz, who wrote about war's violent character – without violence, Rid claims, the term cyberwar becomes diluted and "degenerates to a mere metaphor, as in the "war" on obesity or the "war" on cancer (Rid 2013). François-Bernard Huyghe further accentuates this point, claiming, "a war where nobody risks their lives would be a tournament, a game, a threat, etc." (Huyghe 2011).

Rid also stresses two other elements of Clausewitz important for a campaign to be considered a war – its instrumentality and its political nature. Instrumentality, in its essence, requires a means and an end. According to Rid, in war the means is physical violence or the threat of force. The end then would be forcing the enemy to accept the offender's will. "To achieve the end of war, one opponent has to be rendered defenceless. Or, to be more precise, the opponent has to be brought into a position, against his will, where any change of that position brought about by the continued use of arms would bring only more disadvantages for him, at least in that opponent's view." (Rid 2013).

The third element identified by Clausewitz is war's political nature. "War is always political. (…) War is never an isolated act." In reality, Rid argues, the larger purpose of war is always a political purpose – it transcends the use of force. Rid mentions Clausewitz's most famous phrase; that war is a mere continuation of politics by other means. The author states that the purpose, or the will, of a political entity in a war has to be articulated, at one point transmitted to the adversary; any violent acts and the intention behind them also need to be attributed to one side at some point during the confrontation (ibid.).

To sum up, Rid claims that none of the cyber campaigns that have so far happened have fulfilled all three of the necessary elements. He also remains unconvinced any potential cyber offensive in the future will be able to do so. Rid adds one extra argument to support his claims: according to him, the act of force is a pivotal element of any warlike action – and in most armed confrontations, such a use of force

[4] Cybersecuritynews (2012). For more information about the legal nature of the affair see Schmitt (2013).

is usually more or less straightforward. However, in cyberspace, „the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties". Destruction as the result of a cyberattack would be „mediated, delayed, and permeated by chance and friction" – the attack itself might not be violent, only its consequences.

Rid states that aggression may be criminal or political in nature – he claims that it is useful to group offences along a spectrum which ranges from *apolitical crime* to *thoroughly political war*. He sees political violence (or "political crime") as muddled in the middle; cyber offenses are supposed to be around the middle as well, but Rid perceives them as skewed towards the criminal end of the spectrum. There are allegedly only three activities that result from cyber offenses – sabotage, espionage and subversion. Rid claims that these do not have to be violent to occur or to be effective, nor are they always instrumental. Finally, while the aggressors who engage in these activities might act politically, they usually have interest in avoiding (at least temporarily) attribution (ibid.)

Yet another sceptical voice echoes from Erik Gartzke (2013), who also quotes Clausewitz[5]: "War is not an exercise of the will directed at an inanimate matter". Apart from this jab at the modus operandi of cyber campaigns, Gartzke claims that war over the Internet (sic!) will probably only serve as an adjunct to, rather than an alternative or even substitute to, traditional forms of terrestrial warfare – he literally considers the Internet to be "an inferior substitute to terrestrial force in performing the functions of coercion or conquest". Cyberwar is deemed unlikely to function as an independent domain of warfare – according to Gartzke, most experts view and consider the likelihood of a sovereign nation state being subdued (not to mention falling apart) due to a cyber campaign as "fanciful".

Gartzke rejects the notion that cyberwar might be a revolution in military affairs – rather, he considers the cyber elements in warfare to be a force multiplier, reinforcing the advantages of those countries which are already ahead when it comes to advanced terrestrial warfare. This is tied to his claims that a cyberattack requires the addition of other means of warfare in order to successfully conquer, compel or deter the adversary – Gartzke states that this stems out of the nature of cyberattacks, which are supposedly unable to cause permanent damage – the temporary effect they might have on the enemy will soon be reversed and cause grievances and potentially a response, whose results might eventually mean more losses than achievements for the initiator of the cyberattack.

Such a need to follow up on cyberattacks with traditional kinetic forms of force, as well as what Gartzke calls the "perishability"[6] of cyber capabilities in the face of their revelation, leads the author to a thought that such capabilities are best employed especially with the aforementioned kinetic forms of force – the resulting mode of warfare, paradoxically "most feared by technologically advanced states, may actually pose greater grand-strategic challenges to the technologically backward or weak" (ibid.).

Cyberspace is then regarded as unable to host meaningful political conflict, because it apparently cannot serve the final arbiter function that "has for millennia been the purview of physical violence". In grand strategic terms, "cyberwar (…) remains a backwater". Gartzke criticizes what he sees as a failure to focus on grand strategy – such failure is, according to him, a by-product of the war on terror, "where the objective has been to harm and not be harmed, rather than to effect meaningful changes to the disposition of world affairs".

The main reasons why Gartzke would consider an aggressor to successfully substitute cyberwar for conventional, tangible forms of conflict are that (in accordance to his article) cyberwar by itself cannot achieve neither conquest nor coercion – the cyber capabilities usually do not cause permanent damage, they only disrupt the enemy's capabilities and infrastructure for a period of time. Also, the attacker automatically forfeits the potential to exploit the vulnerabilities (that are being attacked at a given time) in the future – the initiator's adversary then has time to fix these vulnerabilities, and the capacity used for

[5] Quoting Clausewitz seems to be the norm whenever the idea of cyberwar is being discussed – paradoxically by both the alarmists and the sceptics. The alarmists, however, only mention the famous phrase: "War is but a continuation of politics by other means." On the other hand, the sceptics delve deeper into the Prussian military theorist's work, and their claims are usually well-grounded.

[6] Rid also discusses this aspect of cyber weapons (see Rid 2013).

the attack subsequently perishes. Gartzke also explains how deterrence in cyber space can hardly be deemed efficient – the party that wants to deter a potential aggressor has to provide a credible threat, however, once this threat is revealed, even if the specifics are not made available, its potential efficiency becomes greatly reduced (ibid.).

The aforementioned author does not hesitate to also criticize the fact that most of the debate concerning the issue of cyberwar has been directed at the "means" to attack, rather than the "end" – why should a certain nation state come under a campaign of cyberattacks, which would result in a cyberwar? The idea that a certain point of defense is vulnerable should not automatically lead into a feeling of insecurity, he remarks. In spite of this point being debatable, Gartzke perceives critical limitation of what can be achieved through cyberspace – ensuring a lasting shift of balance of national capabilities or resolve simply via the use of cyber capabilities against an adversary might pose a difficulty.

On the other hand, Gartzke disagrees with Rid when it comes to the problem of attribution – in his theory, an attacker who wants to wage a cyberwar eventually will not hesitate to claim the responsibility for the occurring cyberattacks, lest they risk potentially being ignored when articulating their demands. That should be true for both cyberterrorism and cyberwar. "How does one surrender to no one in particular?" (Gartzke 2013).

An Improbable Cyberwar: The Sceptical Standpoint

Firstly, when speaking of cyberwar, a clear distinction needs to be made – taking the information above into account, it seems that when the term is being used, it either indicates the use of the information and communication technologies by contemporary militaries in the pursuit of political goals in the traditional form of warfare, or the new form of warfare specifically being utilized through what is often called the fifth domain[7] of warfare –cyberspace. Arquilla and Ronfeldt (1993) mostly speak of the former; Shimeal, Williams and Dunlevy (2001) distinguish between both of the concepts with Gartzke theorizing about both, while Libicki and Rid (as well as the following evaluation) focus almost solely on the latter.

The reasoning is simple – since information and communication technologies are currently being employed by most of the world's modern militaries; such a "cyberwar" would therefore be almost omnipresent and addressing the likelihood of such would bear next to no meaning. As a matter of fact, the question of whether the simple utilization of these new technologies automatically warrants such a rebranding of the term being used should be raised – the introduction of aircraft to the traditional form of warfare also did not result in it being labelled "aerial war".

With that being taken into account, the likelihood of a cyberwar that would be conducted almost solely through the man-made domain of cyberspace and which would simultaneously comply with the generally accepted conditions required for a conflict to be considered a war (presence of lethal violence, its instrumentality and clearly articulated political purpose, a number of non-isolated incidents with a clear strategy present), at least from the sceptical standpoint, is rather low.

Based on the evaluation of arguments made by some of the cyber sceptics (for the many that were not included in this chapter, see Mueller and Friedman 2014), it is clear that the smaller likelihood of a cyberwar occurring stems from the very nature of cyberspace and cyber weapons as well as from the difficulties when comparing cyber campaigns of the past few years to examples of "classical war" (or even the modern one, for that matter), which is often perceived as a political phenomenon with clearly identified sides taking attributable actions, having articulated goals and a deducible strategy.

While information and communication technologies, computer systems and networks can be utilized as a component of the traditional forms of warfare to a great benefit of respective militaries and armed forces, where the cyber component becomes a significant force multiplier, the potential of the utilization of exclusively digital means to achieve political goals remains limited. There were only a few

[7] After the four traditional ones: land, sea, air, and space.

incidents in which cyber capabilities were employed to cause physical harm – as of this writing, there is no clear proof that any of these incidents directly resulted in but one casualty.

And even if one could cause serious damage, which could even result in significant losses of human lives, the potential to coerce or conquer an enemy, according to Gartzke, remains negligible. Considering further limitations caused by the perceived propensity of cyber weapons to perish, the idea of a non-isolated campaign involving predominantly cyber instruments as weapons seems improbable. This may potentially be subject to change in the future; especially with the introduction of many more automated systems[8] and networks, specifically concerning critical infrastructure[9] and other spheres of human lives (such as transportation and so on[10]).

Due to the limitations discussed above and whilst taking the low likelihood of a cyberwar being conducted on its own into account, it must be said that cyber capabilities are here to stay – they will keep on developing, and may eventually become even more threatening. On the other hand, so will the defence. A much more plausible form of a future war is therefore probably one incorporating cyber capabilities along the kinetic forms of warfare, as well as potentially other forms of achieving political goals.

Conclusion

The text above is but an introduction to the critical approach of the cyber sceptics, which offers a valuable reflection for the debate on some of the contemporary cyber challenges, be it by pointing out the disproportionate securitization of certain cyber threats and by targeting some of the weaker points that have been made by others while trying to tackle the emerging cyber issues in the past few years.

Whether or not a cyberwar will ever take place remains to be seen, from a sceptical standpoint however, the likelihood of a full-blown cyberwar remains low for the foreseeable future. On the other hand, with the constantly changing cyber security environment, this expected projection might be subject to change. This is caused by the ever-increasing reliance of our societies on the functioning of our critical (information) infrastructure, which remains vulnerable to both intentional and unintentional cyber security incidents as well as the growing sophistication of cyber weapons.

These vulnerabilities might pose an even greater risk with the recent emergence of the so-called cyber-physical attacks, the first of which was the infamous Stuxnet worm[11]. Even if such attacks ever result in serious physical harm or even substantial loss of human lives, the objective reasons stemming from the very nature of cyber weapons limits the potential for a fully digitalized war to occur (with such a conflict likely failing to meet the requirement of a certain number of casualties or these incidents potentially being isolated), not to mention achieve designated goals. A rigorous and widely accepted definition of cyberwar needs to be made, for the lack of such a definition may cause serious legal and diplomatic trouble in the international arena.

For the imaginable future, cyber weapons are likely to stay an adjunct to the existing instruments one can resort to when waging war, instead of becoming their substitute. The cyber component will play an increasingly prominent role in military campaigns across the world, but merely as an enabler or a force multiplier, not a significant instrument of its own.

[8] As an example, developments in the field of robotics might be especially fascinating – and also exploitable.
[9] Mr. Kypr, an official with the Czech Ministry of Foreign Affairs, recently noted that virtually all critical infrastructure is being run by information technology nowadays and therefore remains vulnerable in potential cyber security incidents (Maďar and Rezek 2014).
[10] The potential utilization of driverless cars (BBC 2014b), robots serving different purposes, or even the spread of UAVs in the militaries might also entail more vulnerabilities to exploit.
[11] For more on the Stuxnet worm, see Langner (2013).

Cyberdeterrence[12]

Lucie Budirská, Petr Suchý

Introduction

Cyberdeterrence is still quite a new concept, which connects two older topics – the concept of deterrence, which was most prominent during the Cold War, and the issue of cyberspace, which is relatively recent and increasingly important. Cyberdeterrence is one of the topics, which emerged in the academic, military and public discussions at the turn of the 20th century. It is a topic that connects several fields – international relations, security studies as well as information science and computer or IT sciences. If we talk about cyberdeterrence in the context of international relations we connect this topic mostly with discussions about the changing character of war (CCW) and about the revolution in military affairs (RMA).

Debates about the changing character of war result from new or rehashed phenomena, which appeared after the Cold War – namely globalization, decline of nation states, strengthening of non-state actors, rise of new threats (e.g. terrorism) etc. (Sheehan 2011: 216–217). These phenomena have their importance for the concept – for example cyber means facilitate global connections of the world; the cyber environment is not completely controlled by nation states, however it creates opportunities for non-state actors; and many current threats have its reflection in cyberspace (e.g. terrorism – cyberterrorism).

The revolution in military affairs is also connected to cyberspace. The RMA supposes that technological superiority will be crucial in future conflicts. These technologies may be very well connected to cyberspace or even be dependent on it. However, in the context of RMA we must take into consideration that first debates about RMA took place in the USA, which increased the focus on technologies. According to Sheehan, debates about RMA are slowly being replaced with debates about asymmetric forms of warfare in which dependence on technologies may even be a disadvantage. (Sheehan 2011: 220–221)

If we think about the revolution in military affairs in connection to cyberspace, one key question will arise. Is there a possibility that cyber capacities will be crucial for victory in conflicts and that those cyber capacities will determine the distribution of power in the world? So far, there is no proof that the influence of cyber capacities will be decisive and there is real probability that no such proof will emerge. Consequently, we can easily compare discussions about the influence of cyber means with discussions about the importance of aviation which were in motion at the beginning of 20th century – see for example Garden (2002). Particularly the argumentation of Giulio Douhet, the Italian general in the 1920s, shares many similarities with argumentation of current theorists of cyberspace and cyberpower (among others Douhet talked about the civil population involvement in the battlefield, the possibility of attacks on national institutions and infrastructure, and about the importance of prevention).

So why is it important to talk about cyberspace, cyber capacities, and cyberdeterrence if we suppose that cyber means will not be crucial for the world's distribution of power (like nuclear weapons or conventional armies) and will not secure success in future conflicts? It is mainly because cyberspace penetrated into everyday lives of the majority of people in the Western world and critical infrastructure and military capabilities start to be dependent on it.

Cyber and Deterrence "Theory"

Cyberspace Theory

When we talk about cyberdeterrence, we need to first pay attention to the theoretical concepts of cyberspace and deterrence. The word "cyberspace" was first mentioned in William Gibson's

[12] This article is a shortened and revised version of the master thesis "Cyberdeterrence" submitted and defended in January 2014 at the Faculty of Social Studies, Masaryk University.

Neuromancer in 1984. The meaning of this word was a "consensual hallucination". Yet despite the fact that the term "cyberspace" is relatively new, its meaning changed very rapidly since 1984. Unfortunately, the development did not lead to the creation of a unified definition – on the contrary, the understanding of what cyberspace means differs very much. Most theorists of cyberspace emerged in the Anglo-American environment – already in the 1990s many scientists started to think about cyberspace and its significance. However, even the first definitions differed due to their focus on different aspects of cyberspace. In today's literature we could find possibly hundreds of definitions of cyberspace and many definitions of terms connected to cyberspace (e.g. information warfare, information operation, cyberwar, cyberpower, etc.). For summarization of cyberspace definitions and their focus see Kuehl (2009).

This article uses a definition created by Daniel T. Kuehl. Kuehl studied many definitions of cyberspace and on the basis of his research he tried to create his own definition that would cover different characteristics of cyberspace. According to Kuehl, cyberspace is *"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies"* (Kuehl 2009: 28). In Kuehl's definition cyberspace is framed by the use of electronics and the electromagnetic spectrum and at the same time it requires networks and use of information-communication technologies. Simultaneously, this framing is broad enough and leaves space for future forms of cyberspace.

In the context of cyberspace it is important to underline that this article is based on the Anglo-American understanding of cyberspace and also the chosen definition is in accordance with the Anglo-American interpretation. Besides terminological disputes between western scientists we have to deal with a different understanding of cyberspace in China and in Russia. The fact that the world's leading powers understand the term cyberspace differently has many implications especially for the building of international agreements. If three superpowers cannot find a consensus on what cyberspace is, it is very hard to close an international agreement dealing with problems connected to cyberspace.[13] It can be surprising that it is Russia which is active in the international discussion about cyber topics and tries to push towards a united understanding. According to Thomas, Russia is an active participator in discussions about definitions of constituent terms in the UN and in other international organizations. He concludes that Russia tries to be the driving force of international opinions in information-technological topics (Thomas 2009: 487).

The main difference between the American and Chinese/Russian approach towards cyberspace is the usage of the word "cyber". China and Russia prefer their own term "*informatization"* (also a term *"electronification"* is sometimes used in Russian documents). Despite the fact that Chinese scientists admit that their term is synonymous with "cyber" and Russians sometimes use the word cyberspace itself, their effort to create a different terminology is connected to their attempts to cut themselves off the main Anglo-American school of thought. Thomas notes that the main features of Chinese strategic cyber thought are efforts to control the networks and accent on pre-emption. China perceives cyberspace more as a threat for the state and for the party than as a positive tool, an instrument of liberalization. From a military point of view, cyberspace is seen as a new battlefield and as a great new tool for the army. The Russian approach towards cyberspace is also influenced by the feeling of threat towards internal stability. Russia also reflects cognitive aspects of cyber topics. Russian fears connected to cyberspace are often related to the possibility of an information war; information influence on decision-making etc. (Thomas 2009: 467, 476–477).

Security topics connected to cyberspace are also closely related to geopolitics. The geopolitics of cyberspace brings forth many interesting questions and issues. The most important ones refer to whether

[13] Apart from the different understanding of cyberspace there is one other obstacle which hinders international deals. It is a problem called "mirror-imaging". Witlin (2008: 89) says that mirror-imaging is a certain (usually unintentional) transfer of personal experiences and perspectives into analysis of information and data which should be as objective as possible. In debates connected to cyberspace we can find mirror-imaging for example in ascribing the same understanding of cyberspace to our counterpart.

cyberspace is the so-called fifth domain (next to land, sea, air, and space), or if it is a new battlefield or a new way to wage war.[14] These questions lead us to other topics – for example the delimitation of cyberspace borders.[15] Kramer points out that apart from the "fifth domain question" there is one more important issue – whether it is possible to gain superiority in cyberspace. Kramer argues that in contrast to sea, air, and space, cyberspace has its special characteristics (similar to land) which make superiority impossible. These characteristics are the number of actors, ease of access, and possibility of concealment. (Kramer 2009: 12)

All of the cyberspace theoretical difficulties mentioned above are important for cyberdeterrence research. However, before examining the cyberdeterrence concept, it is important to introduce the theory of deterrence.

Theory of Deterrence

The basic definition of deterrence says that deterrence is *"the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits"* (Deterrence 2012). One of the main authors dealing with deterrence, Keith Payne, asserts, *"deterrence is a strategy of issuing threats to cause another to decide against an unwanted behaviour…"* (Payne 2008: 17). Deterrence is thus based on the idea that one actor wants to act against the intentions of another actor. The second actor therefore decides to prevent this action by a certain threat, which should deter the first actor from acting.

Deterrence is a concept, which reached its peak during the Cold War (in the form of nuclear deterrence), although it was known for a long time before the 20th century. According to Payne, deterrence is as old as mankind itself – he presents an example of deterrence on a biblical story of Adam and Eve (see Payne 2008: 17). Deterrence is usually based on one of the two basic threats – punishment or denial. Payne and Walton describe both types. **Deterrence by punishment** is undergoing in case that one actor is trying to signalize to the second actor that if he acts in a certain way, first actor will respond with destroying targets which second actor highly values. If the threat introduced by the first actor is sufficient, the second actor will be deterred. **Deterrence by denial** is based on the same mechanism, yet the threat differs. First actor threats the second actor that if he acts in a way he does not want, the first actor will deny him reaching his targets. These two types of deterrence can overlap or they can be used at the same time. The threats are mostly focused on the so-called counter-value or counterforce targets. Counter-value targets cover cities, economic infrastructure, etc. and they are usually connected to deterrence by punishment. Counterforce targets are military powers, weapons of mass destruction (WMD), etc. and they are connected to deterrence by denial (Payne, Walton 2002: 161–163). Both deterrence by punishment and deterrence by denial can be applied to cyberspace as well.

According to Paul, the deterrer has to fulfil three requirements for the successful pursuing of deterrence: (1) sufficient capacities for deterrence; (2) a credible threat; and (3) the ability to communicate this threat to the opponent (Paul 2009: 2). These three requirements (with some modifications) appear in most deterrence theories (see Payne 2008: 18). Again, these requirements are also valid for cyberdeterrence, which will be examined below. There are some other deterrence assumptions; nonetheless these assumptions are often criticized. The core of the critique lies in the fact that deterrence theories often take these assumptions for granted. Paul (2009: 5–8) mentions four such assumptions – for example the first assumption of deterrence claims that states are rational actors and that they use a calculation of expenses and profits when deciding whether to enter into a conflict. The theory supposes that if the expenses are higher than the expected gains, the state will not enter the conflict. This assumption is the most criticized part of deterrence theory because actors often enter a conflict even if

[14] Again, we cannot find a consensus among authors dealing with these questions. Speaking in favour of cyberspace being a fifth domain are (among others) Gregory J. Rattray (2009) who compares all five domains; David J. Lonsdale (2003) who speaks about the so-called *"infosphere"*. Standing against this argument we can mentionfor example Thomas Rid (2012) who asserts that debates about war in the fifth domain are counterproductive.

[15] For more information about creating borders in cyberspace see Schilling (2010) or Demchak, Dobrowski (2011).

their chances of winning are low and expenses are high – for more details see Paul (2009: 6). Such assumptions bring many questions about the relevance of deterrence theory (e.g. Is deterrence still primarily the matter of nation states? Can deterrence take place among actors, which are not considering open conflict or even war? Are there any deterrence alternatives?), which are connected to the main cyberdeterrence issues.[16]

Cyberdeterrence

Cyberdeterrence is a new concept that combines deterrence with new challenges that cyberspace brings. It is important to mention that when talking about cyberdeterrence, we are referring to deterring cyberattacks, not deterring by the use of cyberattack (even though these two things can overlap in some cases). First pieces of work dealing with the cyberdeterrence topic emerged at the beginning of the 21st century. The main authors covering this topic are from the USA – Martin C. Libicki, Eric Sterner, and Richard Kugler. This is understandable as the USA has one of the most developed cyberspace policies and it also started to develop a cyberdeterrence strategy (which will be examined in conclusion). However, before the introduction of cyberdeterrence, it is important to have a look at the question: "What do we want to deter?".

Possibilities for Using Cyberdeterrence

If we think about cyberdeterrence, we can focus on deterring three possible targets. We can deter single attacks occurring in cyberspace (for example DoS and DDoS attacks, usage of viruses, Trojan horses, sniffer and many other ways of attacking and damaging cyber capacities). The second possibility is to deter conflicts in cyberspace (we understand conflict as acts of actors to enforce their values and interests which are incompatible). We can also try to deter cyberwar.

Cyberwar is a very complicated concept, which influences the whole idea of cyberdeterrence. Basically, authors who write about cyberspace, cybersecurity, or cyberdeterrence can be divided into two groups. The first group of authors believes that cyberwar is possible and it will come soon (or it is already on-going); the second group thinks that the idea of cyberwar is incorrect and that cyberwar is not possible. In addition to this division, there are other, mostly terminological, issues. In the field of international relations we cannot find a consensus about what war is and what its characteristics are. This problem is multiplied in the case of cyberwar. Some authors mark cyberwar as a conflict, other authors mark conflicts as cyberwar. Sheldon writes about the difference between cyberpower being used in a war and between war lead by cyber means (Sheldon 2011).

If we examine a group of authors who believe in the possibility of cyberwar, we will also find a certain distinction. Some authors (e.g. Mike McConnell, the former director of the National Security Agency and of National Intelligence) use the term "cyberwar" for the description of a whole set of illegal or criminal activities which occur in cyberspace every day (including espionage). Yet, only few of such activities labelled as cyberwar can really be included in cyberattacks possibly endangering national security (Sheldon 2013: 307). According to authors who use the term "cyberwar" in this way, cyberwar is already on-going.

Conversely, authors like Chris C. Demchak, Andrew Krepinevich, or John Arquilla and David Ronfeldt believe that cyberwar is a relevant concept and they are inclined to the opinion that the increasing importance of cyberspace changed the character of war. Every hostile incident against some state, some society or economy is a new form of conflict (Sheldon 2007: 307). Demchak claims, *"the nature of 'war' moves from societally threatening one-off clashes of violence between close neighbors to a global version of long-term, episodically and catastrophically dangerous, chronic insecurities that involve the whole society"* (Demchak 2011: 4). According to Andrew Krepinevich, the USA faces a threat

[16] Attempts to deal with the frequent critique and with the question of relevance of deterrence in the world after the Cold War can be seen in modern deterrence concepts - besides cyberdeterrence we can find concepts of extended deterrence (see Crawford 2009: 280–295), complex deterrence (see Paul 2009: 8–9), or well-known tailored deterrence (see Payne 2001: 97, 104–114).

of a "Cyber Pearl Harbor" – a massive cyberattack with little or no notice, which will have serious consequences (Krepinevich 2012: 4). John Arquilla and David Ronfeldt in their warning article "*Cyberwar is coming!"* published in 1993 (!) talk about the information revolution, which will change the way in which societies enter conflicts and also the way in which they lead war. In their opinion, both "netwar" and "cyberwar" are probable and the USA may face conflicts of both low and high intensity (Arquilla, Ronfeldt 1993: 27).

Arguments in favour of cyberwar mentioned above were, and often are, criticized. The most frequent target of critique is Arquilla's and Ronfeldt's article. David Betz reacts to their thoughts with the article *"'Cyberwar' is not coming"* in which he criticizes the whole concept of cyberwar which he sees as a nonsensical neologism which is "strategically disturbing". Betz says that military cyber power is an important supplement of other military capabilities, yet it does not change the nature of war (Betz 2011: 21, 24). Similarly, Thomas Rid argues that cyberwar did not occur, does not occur, and it is highly improbable that it will occur in the future. All past or current cyberattacks connected to some state or government are only more sophisticated versions of one of three activities – subversion, espionage or sabotage (Rid uses Clausewitz's concept of war to support his arguments) (Rid 2013). Thomas G. Mahnken also speaks against the possibility of cyberwar. He claims that the usage of cyber means is still an abstract and undeveloped topic despite many generalizing statements. According to Mahnken, it is not probable that cyberwar or cyberwarfare alone would bring victory or defeat in future conflicts (Mahnken 2011: 57, 63).

What do all these arguments mean for cyberdeterrence? If we talk about cyberdeterrence, we could logically expect a debate about deterring single attacks or conflicts. The concept of cyberwar is still too abstract and opinions about the reality of cyberwar are too competing to think about deterring cyberwar. However, as we will see in the next chapter, many authors connect cyberdeterrence with cyberwar. They do so for two reasons: 1) they believe in the possibility of cyberwar; 2) they are associating cyberwar with conflicts (or even attacks) in cyberspace or with the usage of cyber means in a war.

Concept of Cyberdeterrence

One of the authors who connect cyberdeterrence with cyberwar is Martin C. Libicki. Libicki deals with the topic of cyberdeterrence in his book *"Cyberdeterrence and Cybwerwar"* which is probably the most comprehensive text about cyberdeterrence yet written. According to Libicki, cyberspace is the fifth domain, yet we cannot apply classic historical war constructs (like power, attack, defence, or deterrence) to it, we have to understand it in its own specific way (Libicki 2009: xiii).

Libicki talks about deterrence between states. His emphasis on states is visible in his definition of cyberattacks. He labels a cyberattack a *"deliberate disruption or corruption by one state of a system of interest to another state"* (Libicki 2009: 23). He also limits cyberdeterrence on deterrence by punishment. Libicki especially emphasizes that cyberdeterrence must distinguish perpetrators from the innocent (or good behaviour from wrong). Punishment, which was not deserved, has no legitimacy and creates new enemies for the punisher. It is also necessary that punishment is distinguishable from non-punishment. This is very easy in most environments, yet not in cyberspace. In cyberspace, we are not able to assess the effect of punishment. Therefore, Libicki proposes that if the retaliatory actor is not sure if the punishment will have the anticipated effect, he should consider pretending that no attack occurred (Libicki 2009: 28–30). If we think about Libicki's advice, we will draw a conclusion that this can be a form of deterrence by denial – the victim of the attack prevents the attacker from reaching the target by denying it. The attacker cannot know if the attack was successful and whether the target was reached. This form of deterrence is not realizable in case of attack by conventional weapons; however it may be realizable in cyberspace.

Libicki brings up and answers many questions about cyberdetterence, which are important for creating a credible threat of retaliation – for example: Should the target reveal the cyberattack? When should the attribution be announced? Should cyber retaliation be obvious? In the end of his book he tries to place cyberspace in an imaginary triangle – between disarmament, deterrence and defence. According

to Libicki, the best strategy for nuclear competition is deterrence, the best strategy for conventional conflicts is disarmament, and for cyberspace he chooses defence. Libicki claims that disarmament is impossible in cyberspace, yet defence is inevitable. He sees cyberdeterrence as very problematic and recommends it as a last resort for the American strategy of cyber defence (Libicki 2009: 92–94, 175–178).

Contrary to Libicki's opinion, Eric Sterner claims that deterrence can significantly contribute to American safety in cyberspace. Sterner also focuses on deterrence by punishment and he assumes that the opinion that considers cyberdeterrence to have only little importance emerged from the Cold War interpretation of deterrence. If we want to see all the possibilities of cyberdeterrence, we have to change our expectations. According to Sterner, scepticism about cyberdeterrence emerges from the fact that traditional designs of deterrence have no relevance in cyberspace (particularly the assumption of a bipolar relation of two states with roughly equal powers that want to prevent a [nuclear] conflict at any price) (Sterner 2011: 62, 65).

Sterner admits that cyberdeterrence will never be a key strategy for the defence of cyberspace, yet it can contribute by lowering the seriousness and frequency of attacks. Sterner suggests that the main role for cyberdeterrence is influencing and prevention of spreading and continuation of existing conflicts. It can be used for influencing the opponent's means and goals as well. Sterner also underlines that it is necessary to deal actively with the main cyberdeterrence problems – proportionality, attribution and collateral damage (Sterner 2011: 70, 72, 77). Sterner concludes: *"Over time, a commitment to retaliation for cyber attacks by a variety of means (political economic, military, or cyber) and a willingness to hold cyberspace creators accountable for their role in permitting or enabling attacks will create a deterrent posture. By no means will the United States be able to retaliate for every attack, but visible retaliation will create risk for potential attackers, affecting their cost-benefit analysis"* (Ibid.: 75–76).

Sterner shares his opinion with Richard L. Kugler that the creation of cyberdeterrence is important for the USA. He claims that it is impossible for the USA to completely secure its information networks., yet if the adversary deters, the USA will face fewer risks in cyberspace. According to Kugler, the USA has no such strategy today, however it would be appropriate for it to focus on the conversion of middle-sized attacks to incidents with low probability and deter 100 % of large-scale attacks in the future (Kugler 2009: 309, 326).

Kugler also opposes the argument that cyberdeterrence is unfeasible because of the attribution problem. He claims that the USA needs a strategy of tailored cyberdeterrence. An appropriate combination of motivation tools and physical capacities should stand in the centre of this strategy. Tailored cyberdeterrence should stem from the connection of three deterrence mechanisms: denial, increase of costs, and support retention means, which will persuade the adversary that non-aggression will bring an acceptable outcome (Kugler 2009: 309, 325–329).

It is quite interesting to notice that in the works of these three authors cyberdeterrence is perceived mostly as a threat of cyber retaliation for a cyberattack. In current cyberdeterrence literature, we would find very few references about the possible combination of cyber and conventional means. What about the possibility of deterring cyberattacks by threat of retaliation by conventional (or even nuclear?) means? Or what about the possibility of deterring conventional attacks by threat of retaliation by cyber means? Both options are possible but currently there is very little probability that some state will develop such a strategy. Why? Threat of retaliation by conventional means in case of a cyberattack multiplies some problems mentioned above. In case of a conventional answer you have to solve the problem of attribution. There is also a risk that conventional retaliation for a cyberattack will shift the conflict from cyberspace to the physical world and that it will spin the spiral of escalation. Last but not least, the conventional answer will probably raise a sharp disagreement on the international stage. Deterrence of conventional attacks by threat of retaliation by cyber means also probably won't be used. Success of such deterrence will be small because it is not likely that a state that would like to attack

someone by conventional means would be afraid of cyber retaliation – there is a disproportion that will stop the effect of deterrence.[17]

Can Cyberdeterrence be Effective?

As we noticed above prominent cyberdeterrence authors consider this concept feasible. However, it is also important to raise a question that has so far been neglected – Is cyberdeterrence an effective method of securing cyberspace? Would it be easier and cheaper to focus our efforts on securing cyberspace in some other way? These questions are very difficult to answer because we do not have a generally recognized way to measure the effectiveness of deterrence. The difficulty of measuring effectiveness has its foundations in the basic fact that the goal of deterrence is to deter someone from unwanted behaviour. This means that deterrence is successful when nothing happens. Yet, if a situation does not happen, how can we know that it is due to deterrence? The motivations can be various.

Problems with measuring effectiveness are multiplied in the case of cyberdeterrence. There are many issues connected to cyberdeterrence itself – a high number of actors, difficulties with identification of perpetrators (the attribution problem), frequency of attacks, etc., which hinder the possibility of evaluation of cyberdeterrence effectiveness. In comparison to deterrence of nuclear or conventional attacks there is an even lesser chance to have knowledge of attacks that did not occur. Whereas some steps precede nuclear or conventional conflict (mobilization, movement of armies…), preparation of a cyber attack is usually unnoticed.

At least we can assess if cyberdeterrence fulfils basic requirements for deterrence itself. Paul (2009: 2) and Payne (2008: 17) mentioned such requirements: (1) the message (about deterrence) has to reach the actor (he has to know that he is being deterred); (2) it is necessary to have sufficient capacities; (3) the threat has to be credible. In the case of the first requirement we can say that it is very easy to communicate such a message in cyberspace –cyberspace will spread it itself by its communication means (even to numerous actors). The only thing we have to do is make sure that the actor will pay enough attention to our message. The second requirement talks about sufficient capacities. There are some difficulties here because there is no definite method of measuring cyber capacities of actors in cyberspace (we cannot just simply count the number of weapons or size and state of an army). The answer to the question of what capacities are sufficient for cyberdeterrence will rest on the subjective assessment of the actors involved.[18] The last requirement is the credibility of the threat. The problem of credibility accompanies the whole concept of deterrence, yet in the case of cyberdeterrence it seems to be diminished. A cyberdeterrence threat can be more credible because the cost of possible retaliation (executed by cyber means) is much smaller than in the case of other methods of deterrence. On the basis of this assessment we can come to a conclusion that there is no reason why cyberdeterrence should be less effective than other methods of deterrence. Cyberdeterrence fulfils basic requirements for deterrence and the problems mentioned above (attention, sufficient capacities) are not insurmountable. We can certainly challenge the effectiveness of the whole deterrence concept, however, such a challenge goes beyond the extent of this work.

Conclusion

Cyberdeterrence is still a new and undeveloped concept and there are various opinions on it. There are authors who deny the possibility of cyberdeterrence completely, yet there are authors who see cyberdeterrence as a real option. However, those authors who speak of cyberdeterrence as a real option

[17] On the other hand, there might be a slight future potential in case of deterrence by denial. If there is a threat of attack by conventional means, which are highly technologically developed and dependent on a connection with cyberspace, we can try to deter our opponent by disruption of this connection by our cyber capabilities.

[18] Deterrence capacities are important for one other reason. For example Libicki comes with the idea that better defence makes deterrence more credible. The better the defence, the smaller the probability that attack will be successful and functionality of deterrence will be verified to a lesser extent. And the longer deterrence is untouched, the more credibility it gets (Libicki 2009: 73).

still focus on problems and challenges of cyberdeterrence. There are no pieces of work aiming to design a model of cyberdeterrence applicable in reality. Real usage of cyberdeterrence is also absent. Nevertheless, it does not mean that the cyberdeterrence concept does not have future potential.

At present we can find a reflection of cyberdeterrence in the security policy of one state – the USA. Cyberspace came to American policy in the 1990s – at the time of Clinton's administration. Unfortunately, there has not been great progress on this topic in American policy since – if we compare reports on cyberspace from the 1990s and from 2010s the topics covered are very similar. The first strategy dealing with cyberspace originates in 2003 when Bush's administration introduced The National Strategy to Secure Cyberspace. The most important document connected to cyberdeterrence is the National Military Strategy for Cyberspace Operations published in 2006, which was recently declassified. This strategy mentioned cyberdeterrence as a method of securing cyberspace for the first time. It is only a declaratory mention so there are no practical implications coming from it (as far as it is known). However, this mention of cyberdeterrence signifies that the leaders of the USA have started to think about cyberdeterrence among the methods of securing cyberspace. And we can expect that other states will join this tendency in the future.

Recent developments in American cyberdeterrence policy are described in a "briefing" by Eric Sterner. Sterner follows the speech of Gen. Keith Alexander who expressed concerns about the lack of threshold for retaliation. Sterner calls this problem "red lines" and also points out the problem of uncertainty regarding US cyber capabilities, which creates a gap in the stance toward deterrence. Another weakness of the US deterrence stance is the uncertainty considering unacceptable behaviour in cyberspace. Sterner refers to Alexander's thought that the USA is not entirely sure what such unacceptable behaviour is (Sterner 2014). This implies that there is still a long way towards a practical use of cyberdeterrence.

Jakub Harašta

Introduction

This chapter aims to introduce the legal basis of the principle of distinction and apply the existing legal and scholarly framework to two problematic cases. The initial section introduces both the black letter and the customary legal framework of the principle of distinction and the closely related principle of protection of civilians and civilian objects. The second section applies this framework as précised for the purpose of cyber warfare by the Tallinn Manual in order to determine the point when an information network, hacker, or IT expert become a legitimate military objective.

Law and Its Purpose

The principle of distinction serves as one of the key principles of international humanitarian law (further referred to as „IHL") both in treaties and in customs. The International Court of Justice (further referred to as „ICJ") formulated in its Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons the cardinal principle of international humanitarian law as consisting of distinguishing between combatants and non-combatants and protection of civilian populations and civilian objects.[1] According to the ICJ *„[s]tates must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets"* (International Court of Justice 1996: paragraph 78). This presents the general understanding of the (in)famous principle of distinction within the customary international humanitarian law. Up to date, the application and proper response to newly implemented technology is ensured by the modernized Martens Clause found in Article 1, paragraph 2 of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 1977 (further referred to as "Additional Protocol I") stating, that *"[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."* This is further supported by Article 36 of Additional Protocol I providing that contracting parties in the study, development, acquisition or adoption of new weapons, means or methods of warfare are under an obligation to determine whether its employment would in some or all circumstances be prohibited by IHL. Even the aforementioned Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons outlines that established principles apply *"to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future"* (International Court of Justice 1996: paragraph 86).

The principle of distinction is reflected in Article 48 of Additional Protocol I. In the first part it positively obliges belligerent parties to distinguish at all times between the civilian population and combatants and between civilian and military target, and subsequently direct their military operations only against military ones. Therefore, the civilian population and civilian targets must be respected and protected in armed conflict because the legitimate objective of belligerents is to weaken military forces of its adversary.[2] The principle of protection of the civilian population is therefore understood as inseparable from the principle of distinction (Yves, Zimmermann, Swinarski 1987: paragraph 1911). Until World War I the distinction and protection of civilian populations and targets was unnecessary because the population barely suffered from direct military operations unless it was located directly in the combat zone (Yves, Zimmermann, Swinarski 1987: paragraph 1865). However, World War I changed this course by

[1] Another leading principle is the prohibition of causing unnecessary suffering to combatants, which is irrelevant for the purposes of this chapter.

[2] Originating from the Petersburg declaration of 1868.

implementing artillery with increased range and aerial bombardment. Further changes occurred during World War II. Military operations were directly targeted at civilian populations due to the total war concept changing traditional conflict theories. The state needed to mobilize all of its resources, being material or personal, to wage total war. By implication, the enemy community as a whole became targeted by adversaries (Townshend 2000: 139-141). Therefore, military operations were aimed not only to weaken the military forces of adversaries but also to break his will to fight; war became indiscriminate. Treaties implemented and customs acknowledged after World War II aimed to prevent this state of affairs of indiscriminate attacks from returning in future conflicts.

Aiming to distinguish between civilian and military targets, defining civilians and a civilian population is necessary. Article 50, paragraph 1 of Additional Protocol I defines civilians negatively by stating that a civilian is every person who is not:

- a member of the armed forces of belligerents, as well as member of militias or volunteer corps forming parts of such armed forces (Convention relative to the Treatment of Prisoners of War (further referred to as „Third Geneva Convention"), Article 4, paragraph A (1));

- a member of other militias and members of other volunteer corps, which includes organized resistance movements belonging to belligerents and operating outside their own territory, even if the territory is occupied; (Third Geneva Convention, Article 4, paragraph A (2));

- a member of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power (Third Geneva Convention, Article 4, paragraph A (3));

- an inhabitant of a non-occupied territory, who on the approach of the enemy spontaneously takes up arms to resist the invading forces, without having time to form with others into regular armed units (under the condition of carrying their arms openly and respecting laws and customs of war) (Third Geneva Convention, Article 4, paragraph A (6));

- a member of the armed force of belligerents directly under command responsible to that belligerent for the conduct of subordinates, even if not recognized by an adversary (Additional Protocol I, Article 43).

A civilian population is legally defined as comprising of all persons who are civilians (Additional Protocol I, Article 50, paragraph 2) and is not deprived of its civilian character (and, therefore, of protection) if individuals who are not civilians come within (Additional Protocol I, Article 50, paragraph 3). A civilian population enjoys general protection against dangers arising from military operations (Additional Protocol I, Article 51, paragraph 1) and individual civilians or a civilian population is not to be the object of attack or of acts or threats of violence primarily aiming to spread terror among the civilian population (Additional Protocol I, Article 51, paragraph 2). Civilians enjoy this protection as long as they do not take part directly in hostilities; if they take part directly they lose protection only for the duration of their direct participation (Additional Protocol I, Article 51, paragraph 3).

The principle of distinction and protection of the civilian population is strengthened by positively stating certain obligations for military operations. Indiscriminate military operations are forbidden (Additional Protocol I, Article 51, paragraph 4). Indiscriminate for the purpose of this prohibition is to be understood as not directed at a specific military target (Additional Protocol I, Article 51, paragraph 4 (a)), employing methods that cannot be directed at a specific military target (Additional Protocol I, Article 51, paragraph 4 (b)) and employing methods that cannot be limited to military targets and are of a nature to strike military targets and civilians or civilian targets likewise (Additional Protocol I, Article 51, paragraph 4 (c)). An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is directly prohibited by law (Additional Protocol I, Article 51, paragraph 5). Attacks shall be limited strictly to military objectives, which are understood as

those targets which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage (Additional Protocol I, Article 52, paragraph 2). This narrow focus on definite military advantage was criticized for paying *"too little heed to war sustaining capability"* (Parks 1990: 135-145). Last but not least, installations containing dangerous forces (dams, nuclear electrical engineering stations, etc.) are not to be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population (Additional Protocol I, Article 56, paragraph 1).

In general the principle of distinction does not aim to prevent any civilian from getting hurt, but plainly aims to minimize the impact of military operations on the civilian population. Some civilian damage is unavoidable (Dinstein 2012: 67) and Article 51 paragraph 5(b), Article 57 paragraph 2 (a) and Article 57 paragraph 2 (b) of Additional Protocol I expressly states that it is forbidden to plan, order or carry out an attack against a military target which is expected to cause collateral damage that would be excessive in relation to the concrete and direct military advantage anticipated. This principle known as the proportionality principle is also acknowledged as a customary rule (Zimmermann 2007: 129-132).

IHL does not require any proportionality to exist between comparative losses inflicted between belligerents or damage caused to their military objectives. The principle of proportionality is not to be understood as aiming to limit casualties in armed forces of belligerents to a similar number. There is no limit in the use of force while engaging with an adversary, but only regarding collateral damage inflicted upon the civilian population (Jensen 2003: 1171). Furthermore, not every inconvenience inflicted upon civilians is relevant for the purpose of distinction, protection and proportionality. Scarcities of food or other essentials might occur but only the loss of life, injury to human beings and damage to property matters (Dinstein 2012: 270). As to what constitutes excessiveness, opinions may diverge. The International Criminal Tribunal for the Former Yugoslavia approached this issue in the case Prosecutor v. Galić stating that *"[i]n determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack"* (International Criminal Tribunal for the former Yugoslavia 2003: paragraph 58). Some even argue that a lack of clear rules for assessing excessiveness turns this into art rather than science (Dinstein 2012: 271) but military manuals in general provide guidance for practical application. Some collateral damage offers quantitative characteristics and can be measured objectively, such as the number of casualties or damage to property. But military advantage may not always be assessed objectively and quantitative collateral damage may be balanced by qualitative criteria, such as air superiority (Ibid.), which further complicates the issue. Certain qualities are required for a possible military advantage as well. Military advantage gained by proportionate attack must be direct and specific, not just speculative and general (UK-MoD 2004: paragraph 5.4.4, letter i)). On the other hand, it needs not be immediate (Ibid.: paragraph 5.4.4, letter j)).

Therefore: planning and carrying out the military operation is possible when the target is identified as military objective and possible collateral damage among civilian population or civilian objects is proportionate to definite military advantage the attack or operation as a whole offers.

Applying Distinction to Cyberspace

Applicability[3] of distinction, protection and proportionality in cyberspace is problematic because cyberspace does possess certain specific features. Cyberspace as such largely deforms the concept of geographical proximity[4], which brings us change similar to the abovementioned introduction of artillery with increased range or long-range air operations. The battlefield moved even closer as the civilian

[3] Applicability here means the proper application of specific norms, not the applicability of law to cyber warfare in general (which is disputed for example by China).

[4] This can be understood as the spatial change of the information society as a whole (Webster, 2006: 8-9).

population is now directly connected to the Internet. Their presence within the area of military operations is now ubiquitous (Lin 2012: 523). Not every cyber operation needs to respect the principle of distinction, as there are cyber operations that are legitimate to carry out even against the civilian population, for example some acts of psychological warfare (Federal Ministry of Defence of the Federal Republic of Germany 1992: paragraph 474). For the principle of distinction to apply a cyber operation needs to amount to an attack under international humanitarian law (Additional Protocol I, Article 49, paragraph I). Once the threshold is reached the principle of distinction needs to be applied on every operation regardless of its form and thus is assumed in the examples set further in this text.

The growing dependency on computer systems is one of the main humanitarian concerns when it comes to military operations in cyberspace. Supervisory Control and Data Acquisition systems (further on referred to as "SCADA") and Distributed Control Systems (further on referred to as "DCS") serve as a link between the physical and digital worlds (Droege 2012: 538) and are definitely vulnerable to outside interference. Furthermore, most military networks rely on civilian (commercial) computer infrastructure and conversely civilian vehicles are increasingly equipped with navigation systems relying on GPS. Geographical remoteness diminishes from the hypothetical battlefield and the ability to distinguish between purely civilian and military computer systems diminishes as well because cyberspace as such is dual-use. Some computers are inherently military objectives (components of weapons or weapon systems) but the majority are not military objectives. But they can become such an objective if used by a combatant (Dinstein 2012: 263) or for military purpose in general. By this feature cyberspace directly undermines one of the fundamental assumptions of IHL: that objectives are largely distinguishable (Droege 2012: 541). Cyber operations can be targeted to purely military objectives (e.g. radar field, C^4ISR capacities) more precisely without producing too much collateral damage compared to kinetic attacks (O'Donnell, Kraska 2003: 158). On the other hand, it is more difficult to foresee the effects of a cyber operation due to the abovementioned possibility of a knock-on effect. Assessing this is possible only through a great level of knowledge about both adversaries' military and civilian critical information infrastructure. This might not be available to military commanders at a given time.

However, the interconnectivity of systems also means that the effect of an attack on a military target may not be confined solely to the target itself (Droege 2012: 538), but a knock-on effect taking down other systems may possibly occur (Jensen 2003: 1178-1179). These inherent features complicate the reasonable applicability of the distinction, protection and proportionality to cyberspace, not mentioning the additional lack of understanding of legal implications of waging cyber conflict by armed forces (Lin 2012: 523).

Further issues arise from these inherent features:

I. When is the system a legitimate military objective and when is damage caused to it excessive?

II. When does the hacker or IT expert become a legitimate military objective?

All these issues are closely related to each other through the principle of distinction.

The system as a legitimate military objective and excessive damage

A) Is the targeted system a military objective?

Firstly, appearing in Article 24, paragraph 1 of The Hague Rules of Air Warfare, a military objective was understood as *"an object of which the destruction or injury would constitute a distinct military advantage to the belligerent"*. Military objectives are currently codified within Article 52, paragraph 2 of Additional Protocol I as *"those objects which by their nature, location, purpose or use*

make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage". Once again, providing comprehensive definitions of used terms is of importance. The object is defined as something visible and tangible (Yves, Zimmermann, Swinarski 1987: paragraph 2007-2008) and de lege lata as not containing data per se (Schmitt 2013: rule 39, paragraph 5).

An object becomes a military objective by nature if it is directly used by armed forces (Yves, Zimmermann, Swinarski 1987: paragraph 2020). Weapons systems are therefore military objectives by nature as well as systems included within the C^4ISR capacities of armed forces. The civilian nature of personnel operating these capacities (government employees, contractors) is irrelevant for the purpose of targeting the system with a cyber operation (Schmitt 2013: rule 38, paragraph 6). This illustrates the novelty of cyber warfare because this issue would not be completely irrelevant in the case of a kinetic attack targeting such a facility.

An object becomes a military objective by location if its geographical area makes an effective contribution to military action of the adversary (Schmitt 2013: rule 38, paragraph 7) and cyber operations may be carried out in order to deny the effective use of the area to the adversary. De lege lata it is legitimate to carry out cyber operation against the SCADA system of a dam in order to release water into an area of strategic importance[5] (Schmitt 2013: rule 38 paragraph 7) and thus denying its use to the adversary.

An object becomes a military objective by use if it is used for a military purpose despite its original civilian nature. If armed forces take over a civilian computer network or server field it immediately becomes a military objective through the use criterion (Yves, Zimmermann, Swinarski 1987: paragraph 2022). If military use is discontinued the object ceases to be a military objective (Schmitt 2013: rule 38, paragraph 10).

An object becomes a military objective by purpose if it intended for future use by armed forces (Yves, Zimmermann, Swinarski 1987: paragraph 2022). Obtaining reliable intelligence is crucial when assessing the purpose of objects (Schmitt 2013: rule 38, paragraphs 11-12).

For the sake of the principle of distinction the abovementioned is sufficient to determine whether an object is a military objective. If it falls within the scope of one of the abovementioned criteria it can be targeted by a cyber operation.

B) Is the targeted system dual-use in its nature?

Given the wording of the principle of distinction in both treaties and customs the coexistence of a civilian object and a military objective is impossible. Therefore, if the system is used for both military and civilian purposes the military purpose prevails and strips the system of its civilian status. Therefore, dual-use systems can be targeted by cyber operations because they constitute military objectives.

C) Is the damage caused proportionate?

The positive answer to the previous question subjects the concrete system to the principle of proportionality. Any operations carried out targeting this system must not cause disproportionate damage to civilians or civilian use of the given system (Schmitt 2013: rule 38, paragraphs 2-3). This once again subjects cyber operations to rigorous intelligence and reconnaissance activities because it might not be always possible to assess the ratio of civilian and military use of the system. Doyle raises an interesting question asking whether a dual-use satellite constitutes a military target when the bandwidth used by the military is relatively minor (Doyle 2002: 158-159). When deciding whether to implement a kinetic or cyber operation in order to achieve a military objective, the cyber might be largely favoured. If we turn to

[5] Of course this operation would be subject to certain limitations according to Additional Protocol I, Article 56, paragraph 1.

the Eritrea-Ethiopia Claims Commission we will find that in the case of aerial bombardment it noted that *"[i]n general, a large power plant being constructed to provide power for an area including a major port and naval facility certainly would seem to be an object the destruction of which would offer a distinct military advantage"* (Eritrea Ethiopia Claims Commission 2005: paragraph 1121). Proportionality was not an issue in this particular claim, but the ratio might be of use here when applying Article 57 of Additional Protocol I. This particular Article states, *"when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be the attack which may be expected to cause the least danger to civilian lives and to civilian objects"*. Targeting dual-use objects by cyber operations might therefore be more proportionate than kinetic attacks. Destroying a facility by kinetic attack is less proportionate then destroying the facility with a cyber operation because it is (of course depending on the location of military objective) less prone to cause collateral damage. Shutting the facility down via a cyber operation would probably occur even more often than utter destruction. Temporarily shutting down a power plant by targeting SCADA/DCS related systems in order to achieve a military objective seems more proportionate than destroying it.

However, absolutely favouring cyber operations over kinetic attacks might turn some of its advantages into pitfalls. Cynically speaking, body counts among the civilian population provide military and political leaders with certain pressure in their countries of origin. Removing collateral damage by turning to cyber operations might remove the "body-count alert" that hangs over the leaders as the proverbial Sword of Damocles. Kelsey states that belligerents may be more willing to target civilian or prevailingly civilian targets when the methods in use are largely non-lethal (Kelsey 2008: 1436, 1439-1441), however, secondary casualties caused by system failure can occur.

An IT expert as a direct participant in hostilities

As to the engagement of hackers or IT experts in cyber operations, the Tallinn Manual sprung vast amount of misunderstanding. More frequently than not, reports announcing that the manual provides justification for killing hackers and hacktivits appeared (Souppouris, 2013; Smith, 2013; Casaretto 2013). The main issue here was the case of Anonymous and the question of whether their activities can subject them to targeted killing for example by using drones.

A) Targeting hackers – yes or no?

The Tallinn Manual explicitly states, that *„[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict"* (Schmitt 2013: rule 20). This rather obvious statement is of great importance for the on-going discussion because the rules contained, including the targeting of hackers, are automatically limited only for the time of war. Targeting hackers in peacetime, outside of an armed conflict, is therefore out of the question. Use of lethal force against a target needs to comply with international humanitarian norms; therefore, even hackers or IT experts engaging directly in conflict are not stripped of protection (Ibid.: rule 13). A clear separation of jus ad bellum and jus in bello is of essence here. As for Anonymous, such a collective cannot meet conditions set in Prosecutor v. Tadić (International Criminal Tribunal for the former Yugoslavia 1997). The Tallinn Manual states that *"network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, and data theft do not amount to a non-international armed conflict. The blocking of certain Internet functions and services would not, for example, suffice to trigger a non-international armed conflict, nor would defacing governmental or other official websites"* (Schmitt 2013: rule 23, paragraph 8). A direct reference to Anonymous is quite obvious here.

As for civilian IT experts engaging in armed conflict, although they are not stripped of a certain amount of protection the situation is completely different.

B) What constitutes direct participation in hostilities?

Article 51, paragraph 3 of Additional Protocol I and Article 13, paragraph 3 of Additional Protocol II both state that civilians enjoy protection unless and for such time as they take direct part in hostilities. For an act to be understood as direct participation it must be a specific act that adversely affects or is likely to affect military operations of the belligerent, there must be a direct causal link and it must be directly related to hostilities (Melzer 2009: 47, 51, 58). Once all the three criteria are cumulatively met a person engaging in such an act is no longer entitled to protection. Cyber operations or operations carried out outside cyberspace aiming to incapacitate such a person are legitimate.

In this case there are several possibilities for a civilian IT expert to operate within an armed conflict. First, one is to conduct a cyber operation directly related to an armed conflict – this constitutes direct participation regardless of the civilian nature of an expert. However, maintaining a network or individual computer does not constitute direct participation, regardless of their later use for cyber operations (Schmitt 2013: rule 35, paragraph 5). Actively maintaining integrity of the computer network facing the on-going cyber operation does not constitute direct participation either. A military operation of the adversary aims to enhance his or her own military capacities. By preventing this attack from succeeding the military capacities of the adversary are not lessened, and, therefore, the threshold of harm is not crossed and the first criterion of the abovementioned three is not met. However, engaging in active countermeasures may be considered direct participation in hostilities. Once the IT expert is not just maintaining confidentiality, integrity and availability of his own system but reaches towards the adversary performing hack-back, he or she is probably directly participating in hostilities. For the time of such direct participation killing is legitimate and does not violate any principle of international humanitarian law.

Conclusion

This chapter introduced the legal framework of the principle of distinction and the closely related principle of protection of civilians and civilian objects. Both these principles can be applied to cyberspace without the necessity to adopt new legal instruments despite the fact that certain inherent features possessed by cyberspace may turn this application rather complicated. Despite the positive answer to the application of these principles in cyberspace and clarification of the targeting of information systems and hackers/IT experts, several issues still remain. Firstly, determining the proportionality of an attack when targeting a dual-use network emphasizes the intelligence and reconnaissance and these activities may not always be possible to carry out on the operational and/or tactical level. Secondly, the hackers and IT experts may be directly participating in hostilities without intent and without being aware of it. When performing hack-back the expert is directly participating in hostilities and, yet, he may not know that the cyber operation was carried out by armed forces or the adversary due to the problem of attribution. These issues should be discussed in the course of future research. However, the rules are probably going to remain self-applicable. As in the case of Stuxnet in 2010 or attacks against Georgian infrastructure in 2008, these issues are to be considered before actually deploying the weaponized software itself, but with the problem of attribution in cyberspace violation will only scarcely lead to any sort of sanction.

Alena Leciánová

Introduction

In July 2014 the media informed us[6] about a cyber espionage incident. This event took place in March and its perpetrators were able to intrude the US government network and extract data with information of thousands of employees, especially those with a high-level security clearance, from the network. This is only one of the cases of attacks aiming to steal data concerning nation states' strategies. Most of said attacks are discovered after a relatively long time from the initial intrusion. This fact, besides the possible danger to a nation state's security of course, makes this subject crucial for further investigation, education and prevention. This is also one of the reasons for the author's interest and further research into this phenomenon, mostly called Advanced Persistent Threat (APT). The following article will therefore focus on APT in general – introduction to the phenomenon and its further description, and previous findings of the author concerning the criteria. These findings are the result of previous research conducted while writing the author's bachelor thesis and this article aims to verify these findings using a new set of cases. As a result, this article will not only describe the phenomenon of APT itself but will also bring description of and insight into other cases of APT. At its end, the criteria will be tested.

Previous Research

This article is partly based on previous research of the author into this phenomenon, published as the bachelor thesis "Advanced Persistent Threat: koncept, případy a kritéria" (Leciánová 2013). The objective of the thesis was to create and verify APT assessment criteria and by doing so to also describe the concept and cases of the phenomenon. The criteria are the result of case-analysis and identification of the characteristics specified earlier in previous research (and mentioned below) based on existing literature related to this topic. Part of the previous research and some of the findings will be mentioned and described below.

APT

This part of the article aims to present the context of this phenomenon. The first usage of this term is traced back to 2006 and a group of US Air Force officers (Cloppert 2009, Bejtlich 2010). However, the phenomenon (or the kind of attack per se) might be a few years older, although there is an inconsistency in the debate on how much. The new attack pattern was discovered by American and British experts in 2005. American CERT and British NISCC (later CPNI) published reports in which they distinguished the attack characteristics, which were unlike any of the known attacks (US – CERT 2005, CPNI 2005). The malware was able to bypass any known antivirus software and firewalls and therefore fulfil its objectives. It was also different from other phishing[7] attacks in the aspect of more accurate targeting[8]. To be more specific, the attack was aimed at individual employees' computers and then spread to the whole computer network, targeting mostly governmental organizations and big corporations (Ibid.).

That was probably when experts realized that there was another type of attack that would request their elevated attention and a new set of countermeasures. However, the year of the mentioned discovery was probably not the year of creation and the first pioneering attacks of this type. One of the early

[6] See for example The Washington Post (Barbash and Nakashima 2014).

[7] Phishing is a method of creating and sending fake emails to potential victims in order to deceive them and make them to think the e-mail came from a legitimate organization, for example a bank institution (e.g. McQuade ed. 2009, Watson, Holz and Mueller 2005).

[8] More accurate targeting is a method called spear phishing. In this case, more precisely designed e-mails are created and then sent to victims (e.g. RSA 2011).

examples of the phenomenon (to be mentioned below) is an attack called Titan Rain, which was discovered in 2005 and dates back to 2003 (Thornburg 2005). Moreover, an attack from 1999 was also mentioned in previous research, as some of the experts (Bodmer et al. 2012) also consider it an APT example.

Why APT?

An **A**dvanced adversary is a sophisticated adversary; this includes experience, skills, tools and instruments. R.Bejtlich (Bejtlich 2010) adds that an adversary's advancement can be the adversary's ability to conduct attacks using publicly accessible, trivial tools, including known vulnerabilities and exploits. However, the advancement also lies in the adversary's large resources. These resources enable the adversary to purchase or develop the mentioned vulnerabilities and other highly sophisticated tools. Another group of authors see the advancement as the ability to adapt to a victim's behaviour and as access to limitless resources (Andress 2011, Command Five Pty Ltd 2011).

A **P**ersistent attacker (threat) like APT is able to stay in the system for months or years and be very hard to detect and remove once detected. That is due to ,precise and sophisticated engineering of the malware, and the anatomy of the attack itself (see below). The presence in the network is necessary for reaching the attacker's objectives and/or performing activities in favour of mission completion. The attacker may also stay in the system undetected at low level of interaction, awaiting the right moment or data to come up (Bejtlich 2010, Andress 2011).

A **T**hreat as dangerous as APT owes its dangerousness to the technical sophistication (caused by precise engineering and large resources), which is much bigger than that of more common attacks, e.g. cyber criminal ones. The danger lies also in the fact that this attack is not fully automated and self-replicating but partially driven by a human operator who can adapt to the actions of the victim in favour of successful progress. This is supplemented by a high degree of organization and motivation (Bejtlich 2010, Andress 2011). Last but not least, the fact that the attackers aim for sensitive data of high strategic value, exploitable in other possible attacks, cybernetic or conventional, also proposes that the term 'threat' is used.

Criteria

We isolated valuable criteria for previous research from the above-stated, In the following paragraphs reasons for choosing the criteria will be described, partially using previous research statements (Leciánová 2013).

Resources

In the paragraph regarding the advancement of the attack experience, skills and relevant tools were described as necessary in order of the attack being advanced and hence successful. Bejtlich (Bejtlich 2010) says that the adversary may use trivial tools and publicly known vulnerabilities to achieve its goal but might also reach for example for new and more sophisticated tools and zero day vulnerabilities. These can be designed and found by a team of attackers or simply just bought. In both cases, it is necessary to spend a large amount of financial resources, either to pay the team's 'salary' in order to incite its motivation or in order to pay for 'the goods'[9]. The almost limitless resources implied by the statements above may presumably be related to the state sponsoring[10] the attack (Leciánová 2013). Nation states then

[9] Trade with vulnerabilities and infected networks (botnets) or other tools is not unusual. For example, Jeanson Ancheta was able to make more than 100 000 USD (see Wilson 2008).

[10] This feature may also be shared with cyberterrorism, which may sometimes also be sponsored by a nation state (see DoS 2013), however, both types of attacks can simply be distinguished by taking the attacker's intentions into consideration (see below). Equally, state sponsoring of cyber crime falls within the category of APT rather than cybercrime per se (Leciánová 2013).

use the attacks to exfiltrate strategically valuable data exploitable as a strategic advantage in a possible future conflict. The nation state also exploits the fact that it can only hardly be linked to the attack. The above-mentioned is also the reason why this indicator will also be identified in the case of substantiated assumptions about state sponsoring.

Targets

The direct targets or victims are the individual network users. This and the previous research are focused on the targets more generally, that is on the bigger scale, mostly on the whole of the entities whose networks are under attack (Leciánová 2013). By those we mean organizations (or individuals) possessing and processing information that can be exploited strategically in favour of a nation state, i.e. networks of governmental organizations, defense industrial base[11] companies, activists or simply just organizations or individuals whose information is necessary for the next phase of attack[12]. The targeting itself can in a sense distinguish APT from other kinds of cyber attacks; however, a look at the attackers' intentions is necessary.

Intentions

As stated above, identifying the targets is one of the main ways to distinguish APT attacks from other types of cyber attacks. However, this cannot be done without identifying the attackers' intentions. Let's illustrate it on the following hypothetical cases:

A) The adversary attacks a governmental organization's network and its objective is to 'take down' the network in order for it to be non-operational not only for the employees but also the potential website visitors.

B) The adversary attacks a banking institution's network and its objective is to monitor a particular individual's network for gaining information superiority and/or preparation for another possible (phase of) attack.

In case A we can identify the adversary's behaviour pattern as one we would expect, for example, a hacktivist to adopt. In case B a banking institution is being attacked, however, the adversary's aim is not financial gain[13]. As one can see, the identification of targets is not sufficient to distinguish APT from other attacks. Other attacks may be conducted for example as acts of cyberterrorism or cybercrime. The fact that the intention of cyberterrorists is to achieve their objectives through physical damage and inducing fear (Lewis 2002) and the intention of cybercriminals is mostly financial gain, helps in the distinction of APT, within which the adversary's intentions are to exfiltrate strategically valuable data and stay undetected (Leciánová 2013).

Skills and Experience

Explaining the word 'advanced', it was mentioned that APT is very advanced thanks to both its sources and technical skills and experience. We already focused on sources of the adversary and now we will continue with skills and experience. These features are usually projected into the malware itself and thanks to that the adversary's sophistication[14] may be observed. The observation results are positive when a high level of skills and organization, unlikely those of common hackers, are identified (Leciánová 2013). It is the sophistication of malware engineering (the code) that enables almost impossible detection

[11] A defense industrial base is, according to the US definition (Joint Staff 2013), a worldwide industrial complex of Department of Defense, government and private sector entities with capabilities to perform research and development, design, produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

[12] Organizations and individuals of no first apparent importance will be examined ad hoc according to the circumstances of the attack.

[13] This pattern of behaviour can be seen in the case of Gauss (see below).

[14] Clement Guitton and Elaine Korzak focus on the term "sophistication" and the discrepancies in using this criterion for attribution in more detail (Guitton – Korzak 2013). However, for the purpose of this article, we will work with the perception of this criterion from the previous research of the author.

in and removal from the infected system. This sophistication feature is also one of the ways of distinguishing APT from cyberterrorism and cybercrime. The former aims to be detected in order to gain the stated objective. The latter, although its intention is not to be detected like APT, does not usually use precisely engineered tools but uses the trivial ones that will suffice (Ibid.).

Persistence

The attack persistence is closely related to the skills and experience of the adversary and is one of the main features of APT. By the 'duration of the attack' we mean the period since the first system intrusion, first C2[15] servers' activity and other indicators specified ad hoc by experts (Ibid.). Regarding information about the duration of other types of attacks[16], which is much shorter, usually days (Leciánová 2013, Prolexic 2012), a three-month period (for more certainty) necessary for APT distinction has been determined. However, the assessment of this criterion must be conducted ad hoc regarding other criteria and the circumstances of the particular attack. The discrepancy in the matter of persistence may be seen in the case of Icefog (see below).

Behaviour pattern

Discussing the term 'threat' above it was mentioned that it is the attacker's behaviour, among others, that makes the attack more dangerous and more difficult to detect. The behaviour is controlled not only by precisely engineered software but also by the actions of human operators. This behaviour may be similar to that of military operations, mostly in the sense of high level of organization and preparation (Leciánová 2013). The adversary usually acts in several phases in which a certain modus operandi is adopted and followed. This modus operandi is based on particular tactics, techniques and procedures (see below) and use of relevant tools. The anatomy of the attack will be explained below, describing all the tactics, techniques and other features different from other types of cyber attacks, as this paragraph only discusses the reason why this criterion is chosen.

APT Not State-sponsored?

The issue of the state sponsoring an attack may be considered the most debated, mainly due to the problem of reliable attribution. This is especially true when dealing with issues of a cybernetic nature and origin. Experts in this field have yet to discover a mechanism or a set of guidelines that will help to attribute the attack to a specific actor with no less than 100% certainty. That is why not only the professional but also the general public still raises questions such as: "Why and how can you be so sure that this attack was state-sponsored?". The answer is "We never are". Even in this article we never are. However, almost every researcher encounters more or less important limits to his or her work and acknowledges it most of the time. Throughout this whole article, it is continually reminded that the criteria mentioned are to always be assessed ad hoc regarding the circumstances of the given case.

This question is addressed mainly in the paragraph concerned with resources and state sponsoring[17] Questions regarding attribution may be raised after encountering the case of Icefog (see below). Not to get ahead too much in the article, we will just mention that the perpetrators of this attack were called 'cyber mercenaries'. This term suggests the sponsoring by a bigger actor, most likely a nation state. Although this does not generate any uncertainty, the question is "Can this particular APT be considered state-sponsored when its activity is enabled by sponsoring from more than one (nation-state) entity?". The answer may again be derived from the suggestion to assess each case individually; however, this is yet another example of an uncertainty leading to the debate. When attributing an attack

[15] Command and control servers (C2 servers, C&C servers) are used for the communication of the infected machine with the operators. This term is frequently used in the context of botnets (e.g. Radware 2014, Virus Bulletin 2014).
[16] The attacks conducted by cyberterrorists or cybercriminals are not required to last for a very long time, given the nature of both.
[17] The relation between resources and state sponsoring is described in the paragraph 'Resources' above.

geographical location of both the adversary (if known) and the targets, the language used, political circumstances and others are taken into consideration.

Eliminating all the above we are left with the financial aspect of the criterion. There certainly are many either legitimate or illicit organizations (e.g. Rollins and Wyler 2013) possessing a lot of financial resources being able to afford to conduct or sponsor an attack of such scale. However, given the nature of the phenomenon not every one of them could be identified as a perpetrator of APT, except for the ones with other criteria valid, like the intentions and targets. The organization and individuals targeted within the attack and attackers' objectives reflect the reasons of the attack, that is, among others, to gain a strategic advantage in the future most likely for the needs of preparation for a conflict. This criterion rules out other irrelevant actors. The above can be concluded into a statement that even if the attack is not sponsored by a nation-state it is most likely sponsored by other 'non-state yet state-like' actor with objectives similar to the ones of a nation-state actor. It is what the actor wants that makes APT what it is.

Anatomy of Attack

There have been disproportionately many attempts to specify the pattern and the phases of attack, having in mind the time APT has been known (Ibid.). This is partly caused by the nature of APT per se, that is the many phases of the attack. These phases were split into more or merged into fewer phases by various authors, which resulted in more than one, still legitimate, definitions. That's one of the reasons the synthesis of many opinions was done in this article and previous research .

Preparation

As stated above APT actors are very similar to military actors in the sense of high-level organization and preparation. Consequently, the first phase is all about preparation and reconnaissance. The operators collect as much information about the intrusion points – mostly companies' employees and their authorizations, competencies and more – as possible (SecureWorks 2012, Websense 2011). Some authors add that it is possible that even data about the companies' office layout, technologies and means of communication are collected (Command Five Pty Ltd 2011). After reconnaissance the attackers focus on more technical preparation, i.e. registration of the domain, setting up the C2 servers, scanning for relevant vulnerabilities, code building, preparation of phishing e-mails and testing of all the above and more (SecureWorks 2012, Command Five Pty Ltd 2011). According to experts from Dell (SecureWorks 2012), attacking seemingly unimportant targets can also be a part of the preparation phase as gaining more information for the main objective.

Initial Intrusion

After preparation the attackers usually have everything they need to intrude the first node of the network. This may be done through the deception of the victim by spear phishing e-mails usually containing malicious URLs or attachments, which exploit the vulnerability and consequently infect the network. The attackers may also use the technique of social engineering to lure the particular employee's credentials to later infiltrate the network (SecureWorks 2012, Websense 2011).

Expansion

The initial intrusion may be, if the attacker is 'lucky', directly followed by the exfiltration phase. However, most of the times the initially infected node of the network is not the one with access to the targeted data. Yet, this node is then further used to spread the infection and move on to other nodes of higher user competence and better access to more strategic nodes of network (RSA 2011). This is described as the 'expansion phase' and it is conducted with the use of remote access tools (RAT) and C2 servers controlled by the operators as needed and required in order to reach the objective and stay undetected at the same time[18].

[18] This phase may be also called internal reconnaissance and internal intrusion (Mandiant 2013).

Exfiltration

Although some kind of exfiltration of data is being conducted since the initial intrusion, we will describe the exfiltration of the actual data needed to reach the objective, in other words the extraction that starts by reaching the node with access to strategically valuable information. Extraction may be conducted using various tactics – quick 'smash and grab' ('hit and run' – see Icefog) or careful 'low and slow' (Command Five Pty Ltd 2011). Once the attacker reaches his objective or his presence is detected a series of steps is undertaken to avoid the company's experts tracing the infection to the creator. This includes deleting the traces or planting a 'red herring' (SecureWorks 2012).

Previous Cases

Previous research of the author described and examined multiple cases for the informative purpose and also for the purpose of verification of the criteria (Leciánová 2013). Research of a total of 9 cases was conducted, eight of which were considered APT cases by a greater part of the expert public. The aim to verify the validity of the criteria was the main reason for this selection. The author's intention was to demonstrate the validity on the first eight cases and the invalidity of the ninth (Ibid.). Regarding methodology, the research was conducted as a collective case study (Stake 1995). What follows is a brief overview of these cases.[19]

The **Moonlight Maze** attack is considered by some of the experts as one of the first APT-like attacks ever (Command Five Pty Ltd 2011) as it was already active between the years 1998 and 2000. Some authors (Bodmer et al. 2012) consider this attack to be an APT without doubt, however, there is not much information about this attack to be completely sure. The attack presumably originated in Russia and was most likely state sponsored (Newsweek 1999).

Titan Rain may be considered as one of the attacks that brought the phenomenon to light. It attacked computer networks of US corporations and governmental organizations between the years 2003 and 2006 (Thornburg 2005). Traced back to a Chinese province, it had attacked organizations with strategically valuable information like Lockheed Martin and Sandia National Laboratories (Thornburg 2005, Wilson 2008).

Malware dubbed **GhostNet**, with origin presumably in China, was discovered in March 2009 by mostly Canadian experts. It attacked almost 1 300 computers (of which one third are considered as strategic points) in 103 countries all over the world (The SecDev Group 2009, Nagaraja – Anderson 2009). Among the organizations attacked were foreign affairs departments, embassies, international corporations, media companies or nongovernmental organizations.

Night Dragon probably originated in China as well. It started in November 2009 with the objective to exfiltrate data from world oil, energy and petrochemical companies (McAfee 2011). Exploiting the vulnerability of Microsoft Windows and driven by operators through RAT, it aimed at the extraction of strategic data concerning mining sites, company infrastructure and SCADA[20] systems (Ibid.).

Discovered in the summer of 2010, **Stuxnet** may be one of the most known cyber attacks to the general public. In experts' opinion (Kaspersky 2010), it may be the first cyber weapon aimed at industrial control systems ever. It was primarily aimed at systems of the Iranian nuclear programme (Ibid.) and was able to take out more than one thousand centrifuges[21] (Albright, Brannan and Walrond 2010). Since the discovery there have been allegations that this malware had been engineered by a US-Israeli team and had been part of the Olympic Games operation (see Sanger 2012 or Beaumont and Hopkins 2012).

---

[19] Not including all of the information relevant to the verification in the previous research. Description of the cases will serve only as a quick overview or summary (for more information see the sources or Leciánová 2013).

[20] SCADA - Supervisory Control And Data Acquisition is a category of computer programs used to display and analyze process conditions. In other words it is a medium between the industrial controllers and human operators (Langner 2013).

[21] For a more detailed, technical report of the event, see „To Kill a Centrifuge" by Ralph Langner (Ibid.).

Flame (or Flamer, sKyWIper, Skywiper…), found in the Middle East, is a type of Trojan horse with some features of a computer worm (Kaspersky 2013a). The malware, the size of several megabytes (CrySyS 2012), started being active somewhere between years 2006 and 2008.[22] Flame is very modular and is built on a platform of the same name, and similarities between Flame and other malware was found (see Leciánová 2013 and paragraph on Gauss below). This malware might also be a part of the Olympic Games (see Sanger 2012).

Operation Aurora, one of the malware attacks more known to the general public, attacked many large corporations, including Google (Google 2010), which stated that other mostly financial, technological and media corporations were attacked as well. The attack presumably began in July 2009 and originated in China.[23]

Duqu, malware similar to Stuxnet and Flame, was discovered at the turn of September and October 2011 by experts from the Hungarian CrySyS lab (Bencsáth et al. 2011). Duqu attacked primarily computer networks of six organizations in eight countries – France, the Netherlands, Switzerland, Ukraine, India, Iran, Sudan, and Vietnam (Symantec 2011). The malware had begun its activities approximately in November 2010 and restored its active status in February 2012, only four months after its discovery (Gostev 2012b).

The breach of the American security company RSA, which produces security authentication tokens SecurID (EMC 2014), was discovered in March 2011. The SecurID authenticators are used by many large corporations, including those belonging to DIB. Obtaining these credentials was presumably only the 'preparation phase' of other possible attacks, like the unsuccessful attack aimed at Lockheed Martin only two months later in May 2011 (Lockheed Martin 2011).

After description and analysis in the previous research, it was concluded that in some cases there was not enough information available to responsibly identify the criteria, i.e. cases of Moonlight Maze (two criteria) and RSA breach (one criterion) (Leciánová 2013). However, regarding the other criteria in those two cases and all the criteria in other cases (except Stuxnet), all of the criteria were met and proved valid. In the case of Stuxnet, only three out of six criteria were met (Ibid.). Verification of the criteria in the previous research enables their testing on new cases, which is the main objective of this article.

New Cases

As was stated above, the previously found criteria will be applied to the new cases and to cases not examined in the previous research. Each case will be briefly described followed by an assessment of the findings.

Red October

The discovery of this attack was announced in January 2013. However, the attack was discovered three months earlier in October 2012 (GReAT 2013a). One of the most apparent characteristics was the similar structure with the Flame malware thanks to its highly modular structure. More than 1 000 malicious files were found in approximately 30 different modules (Ibid.). Therefore, this malware proves to be more sophisticated than other malware like Night Dragon or Operation Aurora. The malware began attacking its targets in May 2007 (GReAT 2013a, Higgins 2013) by sending spear phishing e-mails with malicious files attached to the victims. One of the files was for example an ad for a diplomatic car. After opening the attachment Microsoft Office and Java vulnerabilities were exploited (McAllister 2013, GReAT 2013b).

The experts also found that the vulnerabilities used in this attack had also been used in other, previous attacks. However, the Red October attackers used a different executable file. Although the previous attacks using the same vulnerabilities were presumably conducted by Chinese-speaking operators, it is believed that in this case the operators were Russian-speaking (GReAT 2013a). This assumption is supported by the registration data of C2 servers and numerous artefacts left in the

[22] However, Kaspersky experts traced the (most certain) start of its operation only to the year 2010 (Gostev 2012a).
[23] For more information on Chinese attackers, see the report by Mandiant (Mandiant 2013).

executable malware. Most of the C2 servers were based in Russia and Germany and most of the infected networks were found in Russia, Kazakhstan, Azerbaijan, and other countries (Ibid.). As for the organizations the infected networks belonged to, the malware attacked mostly governmental and diplomatic organizations, research institutes, and trade, oil, gas, aerospace and army companies (GReAT 2013a, Higgins 2013).

The malware was able to extract even particular kinds of data, specifically *.acid, a file type of the ACID Cryptofiler software used by the European Union and NATO (Higgins 2013). Besides the similarity with Flame mentioned above, the malware also proved its sophistication by being able to infect and extract data from mobile devices, network equipment, and removable disk drives (including once deleted files) (GReAT 2013a).

Careto

Careto a.k.a. The Mask is an attack that had lasted presumably for at least 5 years. The C2 servers were shut down during the Kaspersky experts' investigation in January 2014 (GReAT 2014a). The malware's names are derived from the word 'Careto' included in some of the modules of malware and from the Spanish meaning of the word, meaning 'mask' or 'ugly face' (Ibid.). This attack is exceptional in the means of its sophistication and it is considered by far the most sophisticated and complex malware ever observed by experts, more sophisticated than Duqu, Gauss, Red October, or Icefog (Kaspersky 2014a). The malware is highly modular and is custom built to be immune to older versions of Kaspersky products.

Another reason for the high sophistication attribution is the malware's ability to leverage numerous backdoors and also to infect operation systems not limited to Windows but also operation systems by Apple and Linux along with the ability to infect various mobile devices. Careto was also able to exfiltrate data like credentials to access the victim's network 'legitimately' in the future (Kaspersky 2014a, McAfee 2014).

The malware presumably started being active in 2007. It infected computers through spear phishing e-mails with a malicious link to seemingly legitimate websites that were simulated to look like subsections of renowned newspapers like The Guardian or The Washington Post or Spanish newspapers (GReAT 2014a). The aim of the malware was to attack and exfiltrate data from networks of government institutions, diplomatic offices and embassies, research institutions, energy, oil and gas companies, private equity firms, or even individuals such as activists (Ibid.). Regarding the countries attacked, most of the infected networks were found in Morocco, Brazil, United Kingdom, Spain, or France (Kaspersky 2014a). The origin of the attack has not been confirmed yet as Spanish is spoken in many countries and the operation might have been conducted under a false flag (GReAT 2014a).

Gauss

This particular malware is, according to experts (GReAT 2012a, Symantec 2012), related to the Flame malware. That is mainly because of the malware's similar, highly modular[24] and complex structure and the fact that Gauss is based on the same platform as and shares some functionality with Flame (GReAT 2012a). The geographical focus of both malware is also the same – the Middle East. While Flame infected systems mostly in Iran, Gauss attacked computer networks mostly in Lebanon, followed by Israel (GReAT 2012b). As for the type of infected organizations, experts found most of the infected computers within the sector of banking institutions, for example the Bank of Beirut, Byblos Bank, Fransabank, and others (Storm 2012, GReAT 2012a).

The fact that most of the attacked organizations were within the banking sector proposes that the attackers had aimed for financial gain (which hints at cyber crime). However, the attackers' objective was not to commit cyber crime per se, but to steal strategically valuable data and observe the victim's behaviour and financial flow within bank accounts (Great 2012a). Along with access credentials for

[24] The modules are named after famous mathematicians – Gauss, Lagrange, Godel, Tailor or Kurt (GReAT 2012b).

online banking systems the malware extracted information concerning social networks, emails and so on of the victim (Great 2012a, Storm 2012).

The malware was discovered in June 2012 after approximately 9 months of activity (Kaspersky 2012). It is a Trojan able to also infect removable drive disks. The malware also had a built-in 'time to live component', which enabled the removal of all traces after a (previously determined) number of individual infection transmissions from the removable drive disk was reached (GReAT 2012a). The servers were registered at an address in Prague and the whole infrastructure was shut down as of July 2012. However, the infection mechanism is still unknown, just like the reason why the malware contained a custom font named 'Palida Narrow' (GReAT 2012b).

Icefog

This next attack was presumably initiated in 2011 and was found still active as of September 2013. A newer version of this malware called Javafog and its characteristics were discovered and announced by Kaspersky experts in January 2014 (Kaspersky 2013b, Kamluk, Soumenkov and Raiu 2014). Whether Icefog was a persistent or non-persistent attack has been a subject of discussion. The reason for this is the unusual approach adopted by the attackers called 'hit and run' (Kaspersky 2013b). Operators using this tactic perform surgical hit and run action; that is they aim precisely only at carefully selected data staying in the system usually for a few day or weeks, hence the persistence discussion. They leave and clean the system immediately after reaching the set goal (Ibid.). Although there were more individual victims, the targets were being attacked one at a time. However, all of the attacks were conducted presumably by the same operators. Experts (Ibid.) called them 'cyber-mercenaries' or 'APT-to-hire' group. The fact that they stayed undetected for such long period of time supports the validation of the persistence criterion.

Icefog targeted mostly networks of Japan and South Korea. The organizations were mostly governmental institutions, military contractors, maritime and shipbuilding groups, industrial and high tech companies, and even telecom operators and mass media (Kaspersky 2013b). This particular malware infects the victims' network through spear phishing e-mails with malicious attachments or links to malicious websites (GReAT 2013c). After that the attackers exploited Microsoft Office vulnerabilities along with Java exploits on the mentioned web pages and malicious HWP and HLP files[25]. The attackers were then enabled to search the victim's desktop and documents and delete passwords saved on Internet Explorer in order to scan the credentials (Kaspersky 2013b). Versions for both Windows OS and Mac OS X have been found by experts who also narrowed the countries of origin to China, South Korea and Japan (Ibid.).

Turla

This malware is known under many names, some of them being Turla, Uroburos or Snake. Security firms announced its discovery at the turn of February and March 2014. The year of origin has been the subject of many debates and it is dependent on the extent to which experts consider this malware as an independent campaign. Some date its origin back to 2005 or 2006 (BAE Systems 2014) and some specify 2011 as the year of origin (G DATA 2014). This article works with the 'safest' assumption that the malware has been active for at least three years. The sample of the malware has been found in computer systems mostly in Ukraine, Lithuania, United Kingdom, and others (BAE System 2014, Dunn 2014).

The most probable reason for the discrepancy mentioned above is that this malware is somehow related to Agent.BTZ[26] (G Data 2014). The vector of infection was still not known for certain as of March

[25] Document files used by Hangul Word Processor used extensively in South Korea, especially by the government (GReAT 2013c).

[26] Agent.BTZ is a computer worm that infected the local network of the US Central Command in the Middle East. At the time it was considered the "worst breach of US military computers in history" and it took specialist approximately 14 months to remove the malware completely from the network (Kaspersky 2014b). Experts (Gostev

2014, but the experts did know that this particular malware was again very complex and highly sophisticated, hence financially demanding. Therefore, it was assumed that the malware had been designed to attack government or research institutions or companies dealing with sensitive information and other similar high-profile targets (Ibid.).

After months of investigation experts came up with new findings concerning Turla (GReAT 2014b), for example the infection mechanism, which is multi-phased beginning with the so-called Epic Turla and continuing with more sophisticated Carbon/Cobra system backdoors once the malware's position in the network is secured (Ibid.). Epic Turla infected the system via spear phishing, social engineering and watering holes[27]. Experts also identified the malware on a Kaspersky user's computer as of 5 August 2014, which indicates that the attack is still on-going.[28]

Kimsuky

Last but not least[29], this article will examine malware called Kimsuky. The name of this malware was derived from the assumptions that arose within the expert public; that is that this attack originated in North Korea, hence the 'Kim' in the name. Although Kaspersky first spotted the malware in April 2013 (Kaspersky 2013c, Infosecurity Magazine 2013), experts came with an explanation of why the assumptions might be valid in September 2013 after months of investigation (Tarakanov 2013). There are three main reasons to believe that this malware is the work of North Korean attackers.

Firstly, the nature of the infected networks is in favour of these assumptions. Among them were South Korean universities and institutions conducting research on international affairs and producing defence policies for the government, a national shipping company (Hyundai Merchant Marine), and individuals and larger entities related to or supporting Korean unification (Tarakanov 2013, Kaspersky 2013c). As for the second reason, Korean words and characters were found in the code. Last but not least, two email addresses used for communication between the attacker and infected machine were registered under the names 'kimsukyang' and 'Kim asdfa' (Kaspersky 2013c). Besides these reasons, the malware is also engineered to disable only products from AhnLab, a South Korean anti-malware company (Kaspersky 2013c, Infosecurity Magazine 2013). However, other hints pointing at North Korea being the attacker will appear in the paragraph below.

Although the infection vector is not certainly known, experts traced the attack back to Chinese Jilin and Liaoning provinces located close to the North Korean border (Tarakanov 2013). This particular malware was not very sophisticated and it contained basic coding errors. Communication was handled with the use of a Bulgarian free e-mail service (Kaspersky 2013c). The intention of the attackers was to steal strategically valuable data from networks of the companies mentioned above. Kimsuky was able to log victim's keystrokes or steal HWP documents (see Icefog) along with disabling mentioned AhnLab firewalls (Tarakanov 2013).

Summary

An assessment of the introduced information and a summarizing table of identified or unidentified criteria will be presented here for a better demonstration of the findings.

As you can see, the indicator of resources or state sponsoring was identified in all of the cases except for Red October. Regarding this attack, there was no sufficient information to identify the

---

2014) also found a connection between Agent.BTZ and Red October (above), however, not as strong as the Turla – Agent.BTZ.

[27] A watering hole is a new tactic employed by attackers when websites to be most likely visited by potential victims are specified and infected in order to intrude the website visitor's system (Gragido 2012).

[28] Kaspersky experts will publish a new report on this malware. For more information go to www.kaspersky.com or www.securelist.com.

[29] On 20th August 2014 experts from Kaspersky announced the discovery of a new targeted attack, presumably conducted by Spanish-speaking operators (GReAT 2014c). This attack is not included in this article, you may search for more detailed and updated information at www.securelist.com.

indicator with at least some level of certainty. The cases of Careto and Icefog were somewhat on the edge during the assessment due to the uncertainty of state sponsoring in the case of Careto and due to the 'mercenary' argument in the case of Icefog. However, Careto was highly sophisticated and complex, hence financially demanding. As for the case of Icefog, a large amount of resources was necessary to finance the 'mercenaries'.

Regarding the targets of the attacks, all of the adversaries aimed at the types of organizations or individuals specified above and their intentions were to steal strategically valuable data. This statement is valid even in the case of Gauss, the banking Trojan, which might have seemed as an act of cybercrime at first glance.

As for the skills and experience, all of the cases but one – Kimsuky – exhibited a high level of sophistication. All of them also identified as persistent, including Icefog, which has been subject of the 'persistence debate'.

Figure 1 - Identification of APT criteria

	Red October	**Careto**	**Gauss**	**Turla**	**Icefog**	**Kimsuky**
Resources	N/A	1	1	1	1	1
Targets	1	1	1	1	1	1
Intentions	1	1	1	1	1	1
Skills and experience	1	1	1	1	1	0
Persistence	1	1	1	1	1	1
Pattern of behaviour	1	1	1	1	1	1

N/A - information not available, 1 – criterion identified, 0 – criterion not identified

Conclusion

As was stated in the beginning, APT cyber attacks appear ever more frequently and our biggest concern should be preventing these attacks and fighting them once they do occur. This article tries to contribute to the best solution of the issues that come with this phenomenon. For its better comprehension, the phenomenon along with previous research of the author was first introduced and described. However, the main objective of this article was to test the previously found criteria on a new set of cases. As can be seen in the table above the criteria proved valid with only some minor exceptions. Precisely these criteria are considered as the above-mentioned contribution, as these may be used for the identification of potential incoming attacks and for better preparation of targeted users to undertake appropriate measures; and also as one of the many views on the issue. As was stated numerous times throughout the text above, these criteria must always be understood in the context of other circumstances and are more of a kind of guideline, which may be updated and modified should any new knowledge of this phenomenon arise.

That is one of the reasons the main objective of this article was to test the previously found criteria on a new set of cases. As can be seen in the table above, the criteria proved valid with only some minor exceptions. Criteria validated in such a way may contribute to the best solution of the issues that accompany this phenomenon, as they may be used for the identification and classification of future APT attacks.

Chinese Telecommunications Companies as a Threat to Critical Infrastructure: The Case of Huawei

Roman Šulc

Introduction

In contemporary society, a huge segment of the world's population depends on mutual interconnection, which, on different levels, concerns social, economic and technological dimensions. As a consequence, structures like financial markets and distribution networks of many commodities and services including important public services such as electricity, gas and water supply, and road infrastructure are more and more associated with electronically interconnected control mechanisms, which are able to handle their complexity efficiently.

From the (national) security point of view, the importance of this fact is well recognized with concepts like Strategic Information Warfare, elaborated by the RAND Corporation, serving as evidence. The idea of Strategic Information Warfare stems from the importance of certain structures, which are perceived as the backbone of an organised society. With sufficient and persistent interruption of these structures, a given society would be in a state of chaos and could eventually face collapse. Should this theory prove to be true, a state attacked in such a manner could succumb even without the attacker's need for army deployment.

In order to prevent similar scenarios from happening, certain important elements of infrastructure are given special attention. Yet, the so-called critical infrastructure is a somewhat misty term as to the recognition of the dimensions and vital parts of various segments. The myriads of electronically connected devices leave much manoeuvring space for arguments and different viewpoints on which to consider as "critical".

Nevertheless, it is certain that increasingly more infrastructure functions and control mechanisms depend on cyberspace. This "environment", which is roughly perceived as an intersection of the physical and virtual worlds, is getting continuously more attention and has influence on strategic thinking. While some security related concepts like cyber warfare and cyber terrorism in their pure forms mostly sound far-fetched (that is from today's perspective), other associated phenomena like cybercrime and cyber espionage are definitely threats to be reckoned with.

It is hardly surprising that the increasing importance of cyberspace as a platform is accompanied by it being used for national interests. Capabilities and intentions of different states in this respect vary, but from the perspective of the Western world, the position of the most aggressive actor in cyberspace is definitely ascribed to China. Represented by the infamous unit 61486, Chinese military not only conducts espionage for the sake of defence but also for commercial purposes aiming primarily at various forms of intellectual property.

In the context of the aforementioned, major security concerns are related to the rise of Chinese manufacturers, which are taking a major share on the global communications market. Probably the most prominent case in this respect is the Chinese telecommunication company, Huawei Technologies Co. Ltd.[1] This text aims to describe Huawei, its portfolio and strategy, as well as risks that this firm potentially poses to critical infrastructure with the elaboration of key assumptions behind presented security concerns.

Huawei's History and Profile

Ren Zhengfei founded Huawei in 1987 in the Shenzhen region, which was constituted by the Chinese government as the first of the special district economy projects supporting private business

[1] Aside from Huawei, ZTE and Datang are also often mentioned.

conduction. At that time, China was fully dependent on imported telecommunication equipment and many of the firms were reselling equipment from Hong Kong. Unlike many others, Huawei had started to develop its own solutions without the international joint ventures approach and quickly profiled itself as a prominent domestic player on the Chinese telecommunication market with exceptionally high research and development to production staff ratio. The first major success came in 1993 with an in-house development of a high capacity switch and a subsequent military contract on supplying the first national telecommunications network (Ahrens 2013: 2-4).

After domestic success thanks to the brilliant strategy, which consisted of the seizure of rural districts and gaining gradual control over bigger centres, hard work, aggressive pricing and thought-through „bribing" system[2], Huawei had saturated China's market and started to expand business abroad. The first foreign market, which Huawei entered, was Hong Kong in 1996 when it started by supplying network components to Hutchinson Telecommunications. Business expansion to other states including India, Russia, Thailand, Brazil, South Africa, and the USA followed in 2001 (Ahrens 2013: 4-9).

Huawei was supplying its products to other states' critical infrastructures as a common provider among the traditional competition such as Cisco or Motorola, but was getting stronger alongside with China's economic growth. The turning point, which led to Huawei's present privileged international position, was massive backing from the China Development Bank and the Export-Import Bank of China in 2004, which enabled the 70 % cutting down of prices compared to the competition (Ahrens 2013: 9-10). In combination with the on-going financial crisis, which had caused the rise in prices of "standard" products, Huawei began to take the lead ahead of its competitors, and its merchandise was starting to take considerable market share. From this point forward security concerns began to rise and spread rapidly.

Nowadays, Huawei is the largest telecommunications equipment producer in the world supplying the vast majority of the largest telecom operators. Its products and services are used in more than 140 countries by more than one third of the world's population with billions invested in research and development, which is conducted via research and development facilities all over the world (Cri Online 2013).

Huawei's portfolio consists mainly of communication network components and related equipment such as routers, switches and other signal manipulating components, various access points, energy sources, and fibre infrastructure parts (Huawei 2014a). Segments in which these devices may be massively deployed are power generation and distribution, telecommunication infrastructure, healthcare, transport, education, finance and public security (Huawei 2014b). Huawei is also one of the biggest manufacturers of the so-called smart phones.

Assessment of Huawei as a Threat

The main factors behind concerns about Huawei's potential as a threat can be viewed as intentional and unintentional. Both characteristics stem from different premises, though potential harmful results for critical infrastructures can be similar. In both regards, following supporting factors play a role of reinforcing agents with respect to the gravity of potential consequences: the number of Huawei's products in use, security-relevant roles of the products and the firm's tendency to act aggressively and massively merge with other related companies (Abras 2013: 23).[3]

With the intentional threat approach in mind, the primary security related concern is the extent to which Huawei is merely a private company loyal to its customers instead of being a proxy of the Chinese government. The following facts are rather in concordance with the latter.

Firstly, for a company as successful as Huawei is on the Chinese market, a good relationship with the communist party (and thus the government/military) is preordained. After all, the Chinese Communist

[2] Managers of local institutions such as the postal and telecommunications services were given so-called "dividends" from the company profits if they agreed to purchase Huawei products (Ashrens 2013: 5).

[3] The most significant examples of business partners are the Russian mobile operator Yota, British Telecom and various other Telecom branches, 3com, Symantec, Vodafone, O2, SwissCom, and other subjects in Germany, Canada, and so on.

Party's Party Committee is located in the premises of Huawei headquarters (Albert 2012). China surely recognizes the telecommunications sector as crucial for national security[4] and is therefore very restrictive toward foreign companies taking part in building its critical infrastructure (Intelligence and Security Committee 2013: 26). Domestic companies within this domain are also profiting from protectionism in the form of cheap loans and tax support (Lee 2012). Military contracts, research and development grants, government support, favourable policy, and Beijing officials' visits are also quite clear indicators (Ashar 2013: 24-27). The aforementioned with regard to the company's history practically renders the option of other than exceptionally good relations between the Chinese government and Huawei next to impossible.

Moreover, a commonly known fact is that Huawei founder, Ren Zhengfei, worked as a military researcher (from 1974 to 1983) prior to his business career. Zhengfei was long known for his taciturnity and for a man in his position surprisingly little was known about his opinions, visions, and social connections. Furthermore, according to a CIA report, Huawei's chairwoman, Sun Yafang, is a former employee of the Ministry of State Security of the People's Republic of China, which is a local military intelligence service (Gertz 2011).

For a company of such influence, relatively little is also known about its management. Officially, its employees[5] own practically the whole company without any third party, but this opportunity is open only for Chinese citizens. This declaration means very little though about internal power distribution as the aforementioned employees are not able to buy shares, but the company allocates them in dependence on workers' positions and performances. As Ahrens (2013: 11) states, even long time employees are not able to understand how the shareholding system exactly works. Real power is still in the hands of the management, which consists of bodies such as the shareholders' union, which is elected by other shareholders and in turn elects the board of directors. Fairness of the election process is naturally debatable and the so-called employee owned status and the company's non-transparent structure can be perceived as an attempt to cover ties to the Chinese government/military (Saarinen 2010).

While the aforementioned statements show considerable potential for collaboration with the Chinese state apparatus, Huawei representatives are sternly refusing such accusations. On the one hand, subjection of Huawei to the Chinese government was never firmly proved; nevertheless, Huawei's previous conduct doesn't show the company as a trustworthy partner. Aside from bribery, corruption and immigration violations (Roberts 2012), lawsuits from its former business partners Motorola and Cisco concerning the theft of their technologies (Barboza 2011), the company also showed disrespect for international law when it broke the embargo on Iraq, and most likely on Iran, too (Michael 2014, Business tech 2013).

Another dimension is the unintentional threat presented mainly by possible insufficient security of some Huawei products, which was indicated by a report led by the US House of Representatives Intelligence Committee. The exact expression used was "sloppy coding" which leaves some devices more susceptible to potential attacks[6] (Taylor 2012). Whether or not this shortcoming was indeed unintentional cannot be told but the minimal production cost in pursuit of lower prices may be a plausible explanation for this kind of quality shortage. Moreover, as Snyder (2013) states, it is normal that electronic components in question are not absolutely flawless.

In this regard, it is probably worth taking into consideration recent pieces of information leaked by Edward Snowden, who has revealed the NSA's efforts to investigate Huawei's background and potentially use Huawei products as their own espionage devices (Hill 2014). This leads to the assumption that the inherent lack of trust toward the Chinese company concerned, and the wide use of its products

[4] The telecommunications industry is one of the seven "strategic sectors/industries" declared by the Chinese government. These are considered as highly important for national and security interests of the state which contributes to the aversion to foreign presence (Lee 2012).

[5] Or rather, Huawei is owned by Shenzhen Huawei Investment & Holding Co Ltd. which in turn is owned by Huawei employees who thus own both Huawei and the company that owns Huawei (Saarinen 2010).

[6] An expample of such a flaw could be the poor random numbers generator for VPN data encryption, which can be subsequently susceptible to security breach by brute-force attack (Snyder 2013).

and services are making Huawei an ideal subject to misuse for the offensive or criminal purposes by any intelligence service, or other sufficiently capable actor with hypothetical gain that in case of exposure, Huawei becomes a primary suspect.

Character of Possible Risks Toward Critical Infrastructure Definition

Huawei's (or any other actor's with sufficient knowledge and means in general) access to critical infrastructure, its building, and maintenance can be harmful in the following ways. The first group of risks is presented by hardware and software modifications (or intentionally imposed imperfections). So-called backdoors enable monitoring and modifying transferred information against the interests of a proprietor of an aforementioned structure. Under normal conditions, this can facilitate espionage or other criminal activities against a broad set of connected subjects. In a state of emergency or war, various modes of deception and misinformation, which would weaken opponents organization capacities, are conceivable. The second of the related variants known as the "kill switch", is a type of modification which is not only able to misuse given component architecture but directly block its usage which may compromise depending services, which in the Huawei case are for example communication, transport, electricity and water supply and so on.

While possible impacts of hardware and software modifications are indeed serious, this type of conduct (at least in the form of a constant change during production process) is somewhat improbable as both hardware and software modifications are discoverable by reverse engineering and software diagnostics tools, which are able to analyze coding. Moreover, as Snyder (2013) points out, Huawei is also very active on the Chinese market, which would expose its homeland to similar dangers, should backdoors, etc., be incorporated in their products. Besides, a lot of other electronic equipment from reputable producers is assembled in China without dragging any extraordinary attention to this aspect even though the possibility of their misuse by the Chinese is more or less the same as it is in Huawei's case.

Somewhat more relevant is the second possible factor, which is manipulation via firmware updates (Prasso 2011). This method has certain advantages since it enables changes that can be caused and after some time cancelled remotely which reduces risk of detection. This method can also be used in combination with maintenance personnel actions, which bring us to the last, dimension of critical infrastructure disruption.

The previous reference is related to the "human element" which has to be taken into consideration during network constitution, maintenance and repairs. It is common, that in order to achieve compatibility and functionality, other parts of a system must be known at least to a certain extent to the Huawei personnel installing necessary components. The same goes for maintenance and repairs, during which knowledge about system functioning and reactions under normal circumstances is necessary. Furthermore, during these procedures geographic locations and the applied security measures for protection of important system parts and nodes are also compromised (Ferro 2012). Aside from that, during system maintenance and repairs other mentioned or similar sorts of undesirable adjustments can be made. Recent accusations of India against Huawei workers (Livemint 2014) shows that this is certainly something that cannot be underestimated.

Huawei's Current Status

As was said above, Huawei's controversial status is widely known. The company can be found in many intelligence agency reports and some governments are taking precautions against the penetration of their critical infrastructure by Huawei.

Without a doubt, the best example of the starkest stance on Huawei is the USA. After a series of preceding restrictions toward Huawei's planned acquisitions, the U.S. House of Representatives Select Committee on Intelligence has openly expressed that integration of Huawei's products into critical infrastructure is not recommended and that Huawei as a business partner cannot be trusted. This basically rules out any possible participation in contracts for the government sector (Ahrens 2013: 29-30, Snyder

2013). Nevertheless, the company is still active in the USA and to all appearances is ready to "start over" to overcome negative public opinion (Gonsalves 2014).

Australia adopted a very similar approach, which directly banned Huawei from a tender for state broadband network building (Sharwood 2013). It remains to be seen whether or not Australia will adopt the "USA model" or rather give Huawei more leeway as the company is already planning to establish an Evaluation Center in favour of gaining a better image.

Similar, yet a more ambivalent relationship towards Huawei is exhibited by the United Kingdom, whose market is open for Huawei business, but the local intelligence community and parliament are clearly concerned about the connection between Huawei and British Telecom as a dominant telecommunications operator as Huawei is its major supplier. The position of Huawei in the United Kingdom is unique because the first so-called Huawei Cyber Security Evaluation Centre was established here in 2010.

This Huawei-administered institution is, similarly as other facilities of the like, directed by the British government in order to evaluate cyber security threats and protect critical infrastructure objects. The facility also serves to test company products for possible security vulnerabilities and to dispel mistrust towards the company. So far, results in the latter regard have been limited since the loyalty of the centre, which is allegedly under Huawei's control, to UK authorities is being questioned (Kan 2013). Unsurprisingly, at least according to the government's perspective, deeper institutional penetration of UK soil by Huawei with inside access to security systems is not welcome. In this case, it is fully understandable because perhaps most threats, against which Huawei's centre should protect, paradoxically came from China, which is a well-known frequent perpetrator of cyber attacks.

Ambivalence is also characteristic for Huawei's acceptance in India. While the company marked revenues are fairly big and an Evaluation Center, similar to its counterpart in the United Kingdom, is planned (IfsecGlobal 2010, Sharwood 2013), Huawei faces imposed barriers for foreign companies and accusations that company employees are spying on India (Intelligence and Security Committee 2013:25, Livemint 2014).

Rather on the contrary, the rest of Europe, where Huawei had doubled its investments between 2010 and 2013, Africa in general and some Asian and Oceanian states don't seem to be concerned with Huawei's activities on their territories. While the main domain of Huawei in European countries is modernizing communication networks by building LTE and other so-called fourth generation data networks as well as internal communication systems for railway systems (Turkey, Turkmenistan, Norway) (Leadership 2012, Morris 2013), in Africa, many telecommunication and other related infrastructure is built by Huawei from ground-up. The most prominent customers can be found in Kenya, Ghana, Ethiopia, Zimbabwe, and Zambia (Reed 2013). Monumental projects like Konza City and Hope City, which are planned business megapolises, are also wholly dependent on Huawei's technological solutions (AfricaItNews 2013). Penetration of such magnitude, combined with resource-rich and often volatile African governments and Chinese strategic interests understandably raises many concerns about the purity of business intentions of Huawei on the African continent.

Huawei's Strategy

Since the firm's modest beginnings, very little has changed in Huawei's strategy department. Looking at the example of the African market, the tendency to "surround the city with the countryside", which has proven victorious back in China, is clearly illustrated. The second pillar of its strategy, which is to aggressively undercut the competition, is also clearly taking place worldwide as Huawei's prices and special offers have hardly any rivals.

Aside from using "old tricks", a new strategic challenge, connected with the security regards, has arisen. Huawei certainly isn't stoically accepting accusations and suspicions formulated by its opponents. The major line of used counter-argumentation gravitates toward huge revenues which would be at risk should the company take part in some sort of illegal activity against their clients (Reed 2013). Company

representatives also firmly refuse ties with the Chinese military or government and call for direct evidence, which would prove otherwise.

Aside from rhetorical statements, Huawei is also starting to change its code of conduct in favour of bigger openness. Nowadays, Huawei is a little more compliant in revealing the company's organizational structure as is evidenced by the board of the directors' revelation in 2011 (Kan 2011). It is possible that more compromises will appear in the future, at least according to proclamations of Zhengfei's daughter, who has promised further information on the ownership structure (Xia 2013). Yet another of the company's characteristic traits is persistence regarding activities on markets under government restrictions like the USA and Australia.

Probably the most shocking act of frankness support came in 2013 when Ren Zhengfei started to give interviews after a long 26 years of silence. Various security-related topics were covered as Zhengfei stated that he is not a pawn of the Chinese government or anybody else and denied the possibility that Huawei's workers would cooperate should Chinese intelligence ask them to do so. Zengfei also touched upon rather strange subjects as he, aside from other things, admitted that his life would have been better if he had chosen pig breeding instead of telecommunications as his profession (Ibnlive 2013, Crouch 2013).

While the basic elements of Huawei's strategy are time-tested rural and developing-country markets serving as the key to more challenging destinations, and very competitive prices of its products it is conceivable that equal importance belongs to UK-inspired Evaluation Centers, which will be established as a next step in market and public relations control with the most probable candidates for this step being India and Australia (Albert 2012, IFSEC Global 2014). This practice is also connected with another typical element of Huawei's strategy, which is flexibility towards various markets. The hiring of local ex-politicians and ex-soldiers as lobbyists can be mentioned as evidence (Vance and Einhorn 2011).

Conclusion

In a convoluted case such as that of Huawei with a lot of potentially relevant information out of reach within the open source realm, no ultimate clear conclusions can be made. Perhaps the best starting point of this concluding assessment, which defines the boundaries of the inference bellow, is Huawei's indisputable close relationship with the Chinese state apparatus and the fact that none of the aforementioned accusations about the firm's malicious intentions have ever been proven.

Even in the best-case scenario that Huawei is indeed only a business actor and accusations against it are motivated by protectionism, xenophobia and paranoia, perhaps fed on by their own espionage conducting (as Huawei representatives often state), with information about critical infrastructures and access to enormous amounts of data the involvement of Huawei surely presents a risk, because it is easily possible for Chinese intelligence to infiltrate Huawei despite Ren Zhengfei's assurances[7]. This kind of action would be naturally much easier than trying to obtain similar information of such unprecedented depth and magnitude by other means. The often-discussed insufficient quality of Huawei's products, whether it is deliberate or not, can also be problematic, as it has already been pointed out.

The second hypothesis, the plausibility of which is supported by the company's cryptic profile, high-ranking individuals connected with Chinese military and intelligence (Zhengfei and Yafang), army contracts and previous questionable conduct, is that Huawei is to an uncertain extent controlled by the Chinese state apparatus, and while contemporary political goals may be in accordance with purely business interests of Huawei and thus also serve in favour of its clients, the probable strategic goal is to build vast and deeply interconnected infrastructures which can be misused to various degrees anytime by the Chinese government. Whichever of the presumptions is closer to the truth, the same logical conclusion remains, which is that enabling any major participation of Huawei on critical infrastructure is certainly not desirable.

[7] Not only does Zhengfei's statement make no sense, but also in cases of such strategic importance as Huawei is (army contracts, local critical infrastructure building and huge revenues) Chinese intelligence is most likely already well settled in.

Lea Hricikova[1]

Introduction

"Current approaches to cybersecurity are not working. Rather than producing more security, we seem to be facing less and less" (Dunn Cavelty, 2014: np). The environment of such conditions deserves a careful analysis. The exponential increase in frequency, complexity, cost and in general danger that cyber incidents represent is a trend of the last decade. Nonetheless, fears of such incidents have spread across the full spectrum of society and concern the international organizations and the private sector alike, not to mention the states, as the measures set in place by each fall short of the desired effect. The level of interconnectedness increases the number of security incidents and the most interconnected become the most targeted (as is the case of the US). That is followed by an increase in the use of "language of urgency and general doom", a rise in organizing military structures for cyber defence and in cybersecurity defence spending (spending on offence is more an exception). Consequently, more countries take initiatives and measures addressing the whole spectrum of society, despite the overall lack of transparency, or attribution for that matter, in cyberspace (Dunn Cavelty, 2014: np).[2]

The objective of this article is to present the research findings on the potential of the regional cooperative regimes to contribute to security in cyberspace. The research will focus on the normative development that the regional cooperative regimes could facilitate for states and all other stakeholders with vested security interests. At the same, it will identify the drawbacks and the space for improvement in regional cooperation. The feasibility of the regimes setting up long-lasting international cybersecurity norms will also come into question.

Cybersecurity, as used here, is a general term that covers all malicious activity directed at cyber systems and infrastructure amounting to espionage, warfare or crime, either with the intent to destroy the systems or infrastructure, or to preserve it while exploiting it at the same time (Clark, Diffie and Sofaer, 2010: 179). Cyber threats are mostly described as global and international in their reach. However, this article does not focus as much on the global reach of the threats as it does on the commonality of particular threats to particular regions. As other authors pointed out, the treatment necessary to address the diversity of the threats often yields contradictory effects (Dunn Cavelty, 2014: np).

The starting point for regional action and cooperation are principles entrenched in the UN Charter. Chapter VIII Article 52 of the Charter lays legitimacy and the accountability foundation for regional organizations (Fawcett, 2004: 436). The region-specific policy on security ensures cooperation among the state and non-state actors and coordination of a strategy within a given region. This "regionalism" identifies the norms, rules and procedures for its foundation and creates expectations. The process that sets in the establishment of formal institutions is "regionalization" (Fawcett, 2004: 433). As such, regionalism and regionalization indicate the stance toward and the way in which regional actors will address the cybersecurity dilemma. The framework of a security dilemma might prove useful in explaining the complexity of the problem. This would either lead to a cost-effectiveness analysis and a subsequent broad acceptance of emerging norms or to a défilé of insecurities in front of other stakeholders.

The first part of the article will define the cybersecurity dilemma affecting the stakeholders and its dynamics but it will also identify available responses from the normative point of view. The following

[1] "Many thanks to Nathalie and Matteo who are, indeed, awesome and to the experts at the NATO CCD COE for their invaluable advice."

[2] The author proposes the following definition of cyber security: "cybersecurity signifies a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. The related security discourse is about a diverse set of threat forms, ranging from basic computer viruses to cybercrime and cyberespionage activities, as well as cyberterror and cyberwar. Each sub-issue is represented and treated in a distinct way in the political process."

part will hold to account the particular measures necessary for regional cooperation to tackle the cybersecurity dilemma. The third part will introduce findings that are based on the process-tracking of cybersecurity legal regimes in the respective regional organisations and an evaluation of the suitability of the process with measures identified in theory, which will lead to a conclusion in the final part of the chapter.

Importance of Regionalism for Cybersecurity

Security dilemma: The dynamics in cyberspace

In its essence, the security dilemma concerns individuals, organized groups and their political leaders, and the accumulation of security in the international environment. These actors employ their material or non-material measures for the very existential interest but also to avoid the harm or inconvenience to less vital interests. Preventing the impact of security measures of others on one's own security – by using more security measures for one's self – causes the accumulation of insecurity (Herz, 1950: 157-158).[3] The recurrent tension caused by the accumulation of security is inherent in the interaction of sovereign states and induced by the "existential condition of [un-resolvable] uncertainty" (Christensen, 1999: 49).

"Various security needs are not aligned; and while they do not always have to be, more awareness of the clash between them is needed. Referent objects also reveal a lot about (hidden) power structures" (Dunn Cavelty, 2014: np). The willingness to revisit the power structures to satisfy the security needs, especially when not widely shared, adds up to the uneasiness of this environment. That gives the foundation of the security dilemma (Jervis, 1978: 169). However, setting this understanding into cyberspace is more complex. The dilemma in cyberspace "exists when efforts by one state to enhance the security of its digital infrastructure, either through the development of offensive or defensive cyberwarfare capabilities, decrease the cybersecurity of others" (Rueter, 2011: 35).

Similarly, the presence of fear and its impact on decision-makers, underlined by the indifference to the emerging cybersecurity trends that create an environment of mistrust and uncertainty, employs different dynamics in cyberspace. As an example, trust and confidence in the security of the ICT carriers are undermined by the on-going exploitation of computer-system vulnerabilities by national security agencies. Yet, encouragement of such practice does not only impact the trust and confidence but also is a threat to the state itself (Dunn Cavelty, 2014: np).[4] The inability of a sovereign entity to grasp the security risks within its own reach is an additional factor of consideration when interpreting the intentions of other stakeholders (Rueter, 2011: 27). Also, whether the fears as well as the accompanying trends are presented as a "natural" development or as a result of complicated political processes depends on who is asked (Dunn Cavelty, 2014: np).[5] Thus, the specificity of cyberspace, the asymmetry in IT development and the uncertainty and fears constitute obstacles to dilemma interpretations and escalate into a hindrance to any sort of cooperation (Rueter, 2011: 1).[6]

Security Dilemma: The Strategic ambiguity

An additional significant challenge for the phase of interpretation is the persistent presence of the strategic ambiguity of intentions and capabilities. This is a particularly attention-worthy element of the security dilemma in cyberspace. "What becomes exceedingly clear from the developments and lessons of the last decade is that we cannot have both: a strategically exploitable cyberspace full of vulnerabilities—

[3] Herz mentions escaping "the impact of the power of others."

[4] Instead of fixing the cyberspace vulnerabilities (entry points for misuse), they are exploited (used) for the possibility to have better security awareness. An alternative conduct would see a greater focus on the effort to limit the impact of the malicious exploitation by the security agencies, which unlike the original conduct would not reduce the environment of trust.

[5] The latter is more probable.

[6] Jervis (in Jervis, 1978: 62) points out that having various arms control regimes in place and an understanding of the limits of used systems has not improved security.

and a secure and resilient cyberspace that all the cybersecurity policies call for" (Dunn Cavelty, 2014: np). The reason for the ambiguity in place is the pursuit of the outstanding added value to national assets (capabilities, or non-material – intentions) attached to the lack of communication on their purpose. Few strategic papers demonstrate that the states have recognized the opportunity of the mere existence of cyber capabilities transforming the way these states are perceived (Rueter, 2011: 1).[7] Where some see advantages to not having a defined position on cybersecurity, others see a clear position entrenched in international norms, take for example the use of force as pivotal for discouraging and preventing individuals or countries from undermining cybersecurity (US GAO-10-606, 2010: 38).

Interpretation of capabilities

The ambiguity, mistrust and the uncertainty will be mitigated firstly via an interpretation of the material and non-material capabilities of the stakeholders involved in the dilemma, followed by a response (Booth and Wheeler, 2008: 1, 5). It should be considered that next to the material and non-material capabilities the understanding of the decision-maker is equally as important on the personal level. Thus, the interpretation is a complex relationship of psychological and material dimensions (Hollis and Smith, 1990: 13). Meanwhile, the actors who are by design responsible for security continue fuelling the cybersecurity dilemma because of the wide spectrum for interpretation attached to existent cyber capabilities. The "inherent ambiguity of weapons" is undeniable, especially in cyberspace. Thus, the motives and intentions become significantly harder to interpret and the existing military policies as well as legal milestones in the field of cybersecurity are continuously subject to careful global scrutiny for precedents and to a substantial dispute among different interpreters (Rueter, 2011: 23).[8]

The differentiation and verification of offensive cyber capabilities is less possible due to the widespread typically non-menacing platform of their launch. Also, the earlier mentioned nature of cyberspace favours the offensive. The classical mobility challenge is superseded to the offense, taking advantage also of the speed and immediacy. All of these assign a high cost to the defence when compared to the cost of the offense. The cost broadens the scope of the security dilemma in cyberspace to encompass a greater number of actors to whom offensive is affordable. Thus, the offense asymmetry ("easier, faster and cheaper") makes it sufficient to only succeed once against the defence (Rueter, 2011: 32-38; National Research Council, 1999: 12).

Understanding the prevalence of offensive as one of the available attributes of cyber capabilities instead of their determinant corresponds to a security dilemma sensitivity. "Precautionary and defensively motivated measures" are, without the necessary sensitivity, perceived as offensive threats or countermeasures reducing security and strengthening regional tensions. Sensitivity requires attention to the process in capability-development, as well as in decision-making, as opposed to dominant narratives (self-fulfilling prophecies about the danger of one's security environment). Advocating classical deterrence based on unilateral measures, as opposed to international cooperation, is a typical example of disregarding the transnational nature of cyber threats calling for deterrence (Clark, Diffie and Sofaer, 2010: 179). Therefore, the interpretation of cyber capabilities alone is unlikely to settle the fears of using the capabilities (Rueter, 2011: 4, 441).

Response

The second mitigation instance of the security dilemma features a response in words or deeds of a deterrent purpose, aiming again at increasing one's security. As put by Jervis, "many of the means by which a state tries to increase its security decreases the security of others…[o]f course, these measures are not convenient, cheap or certain to success" (Jervis, 1978: 169). The response determines the stance of the stakeholders towards the security concerns raised that caused the dilemma, it will come in a fashion of a

[7] As an example see e.g. the Australian NCSS in United Nations Disarmament, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (in UN Disarmament Study Series 33, 2010: 17).

[8] "Weapons are inherently ambiguous in their politico-strategic meaning; consequently, their very material potential invites mistrust" (Booth and Wheeler, 2008*:* 42-61).

strategic shift in policy and administration and it will end in either an accommodation or an unwanted increase in hostilities. The latter is called the security paradox and is the extension of the security dilemma, yet distinct because of the long-standing presence of hostilities (which is the case of security in cyberspace today). This implies that material capabilities and rhetorical analyses are used to disentangle motives and intentions only for the temporal mitigation of the perceived threat. So are the reform, transformation and trust-building that were meant to address the threat (Booth and Wheeler, 2008: 2, 5, 9).

The accommodation is accompanied by a strategic challenge, a period when the dilemma is settled and during which the stakeholders assess the extent of the accommodation (Booth and Wheeler, 2008: 9). The accommodation in light of the security discourse is a dire political process tailored carefully to the variety of "political, private, societal, and corporate notions of security" to move (mobilize or demobilize) a particular audience (Dunn Cavelty, 2014: np). The wide spectrum of involved stakeholders would downplay the possibility to reach an agreement. A quantity of varying stakeholders tenant to their perception on irrevocable qualities of cyberspace (e.g. accessibility over security) will perceive the security loss as an externality. The unwillingness to pay the price for security downplays the possibility to reach an agreement regionally. This highlights how cost-effectiveness of the accommodating measures is vital.

Yet, it is seen rather in the privately owned profit-generating enterprises that design and define the future of the security and technical standards of the Internet than across institutions, which proved inefficient and sluggish in ascertaining standardization in cyberspace.[9] The cybersecurity standards expanded on a consensus basis, voluntarily and without an enforcement mechanism because their cost-effectiveness demonstrates itself, as it is entrenched in the comparison of the price of negligence and of the employed passive defence based on low level of maintenance and end-user awareness (Clark, Diffie and Sofaer, 2010: 182). The cost-effectiveness is unlikely to be guiding the security standards of all stakeholders for which cyberspace is an environment unsuited to traditional responses to insecurity.

On norms

International norms fell short of accommodating the earlier-mentioned design of cyberspace that provides the basis for the security dilemma (Stevens, 2012: 165). Norms can take years to develop and spread and cannot be unnaturally imposed on other states (else they serve merely as symbolic or idealistic propositions) (Rueter, 2011: 45, 53). Although not always codified in law, norms often inspire or lead to the development of international law. Institutions can help create and foster norms, although norms can also develop at the domestic level and then "diffuse" throughout the international system (Finnemore and Sikkink, 1998: 894; Rueter, 2011: 51). Either way, a precondition for the emergence is a "collective understanding of the proper behaviour of actors" (Legro, 1997: 51; Finnemore and Sikkink, 1998: 891; Rueter, 2011: 2). This also means that norms create expectations to the extent that identifiable patterns of behaviour will emerge, which will influence the behaviour of other stakeholders (Rueter, 2011: 49, Fawcett, 2004:429, 432, 439). The regularization of behaviour "for actors with a given identity" limits the range of their choices and constraints actions, which delivers social order and stability (Finnemore, Sikkink, 1998: 894).[10] The presence of norms is closely associated with not only a platform that institutions provide for the collective understanding but also with the value that the institutions (in this case regional organisations) either produce or stem from.

[9] More on the debate of the delivery of security dilemma accommodation from institutional, rational and liberal actors with a picture of a political and economic causality present in the IR can be found in (Herz, 1950: 195).

[10] The method of this behavioural change has not been settled in the literature, yet an alternative encompassing a number of streams is merged in the notion that the norms provide a "strategic social construction", in which maximizing one's capabilities is used for influencing and changing the function of the capabilities of others, according to the normative commitments (Finnemore, Sikkink, 1998: 910).

The conditions for the emergence of norms

The underdeveloped security institutionalization to counter cyber threats remains a problem (Christensen, 1999: 49). A case in point is the different approaches to cybersecurity that the US and Russia have taken despite their common effort to reach an international consensus on cybersecurity norms (Arimatsu, 2012: 91-94). The United Nations General Assembly (UN GA) drafts on international code of conduct for information security have been submitted by Russia and, among others, China. The early common initiatives signalled that the American and Russian legal perspectives are irreconcilable. Nonetheless, both acknowledge the economy-boosting as well as subversive attributes of cyberspace. The US considered cybersecurity as a law enforcement paradigm, ideally governed through convention and mutual assistance. Since cyber threats are of a criminal nature and not political one, as the US sees it, current law is sufficient to fight malicious cyber activity. Such a stand also allows the country to refrain from forming its position on armament or warfare, and the reluctance to do so is substantial.

On the other hand, Russia envisages "the development of a binding international regime" (entrenching respect for sovereignty, territorial integrity, political independence, and refraining from posing a threat to international peace and security, acts of aggression and information proliferation) (Trenin, 2013: 5-7; Shanghai Cooperation Organization, 2001:2009-5-7). Russia is by many accounts one of the most rigorous advocates of a cybersecurity cooperation mechanism. In this sense, efforts to develop international principles through a UN GA resolution on fighting "information terrorism" are strong. Since this effort was closely associated with information censorship, Russia has repeatedly amended and softened their resolution. Nonetheless, a significant disagreement on the classification of intervention into domestic affairs remains. Russia's pursuit is driven by dependence on commercial security solutions and foreign expertise in view of the presented trends, it is more apparent now that such proposals gain maturity, as cybersecurity becomes a prominent part of national security (Rueter, 2011: 43, 44).

Although no conclusion on these greatly varying approaches to the overarching strategic objectives is foreseen, a substantive escalation is mitigated by a platform that serves the interest of reducing competition, in this case the UN. Furthermore, the case above illustrates that the contradicting ideas on cybersecurity continuously slow down the emergence of a common norm. Thus, facilitating a collective understanding of carefully chosen values requires that the concerns of several stakeholders with varying splitting interest will be mitigated. For this purpose, a regional rather than an international option becomes a first instance of an accommodation.

Benefits and Challenges of Regionalism for Reducing the Security Dilemma

The ever-increasing interdependence and a highly unequal volume of regional cooperation during the institutional development of the 20th century exposed the stakeholders to a variety of cross-border issues. As a response, multilateral platforms with delegated responsibility have emerged on the transnational level with potential for performing efficiently in particular tasks. Yet, the relevance of these regional institutions and organizations has been highly dependent on the "response to both, an internal debate and an outside threat" (Fawcett, 2004: 430, 431). The states as well as the key stakeholders find vital security concern inside and outside of their region. Both have to be addressed, preferably as efficiently as possible by the internal cohesion as well as the ability to expedite outside of the region (existent in the most advanced regional concerts). Cooperation as such allows states and other stakeholders to pursue self-help solutions, yet heading towards mutual security (Rueter, 2011: 31). In this respect, regional cooperation provides a useful platform to address a concerned issue globally, and becomes complementary rather than an alternative to the global approach to address the dilemma of cybersecurity.

As long as the stakeholders share geographical, political, economic, strategic, and cultural concerns, while at the same time they function under the norms, trends values, and practices applied globally, regional interaction will provide a possibility for cooperation. The institutions with their legal regimes applying agreed norms and procedures have been a longstanding platform for reducing uncertainty, helping to articulate intentions to each other and reducing the costs and risks of security

measures (especially when tied to other cooperative measures) (Rueter, 2011: 49, 50). The consent to participate in a cooperation platform (or an agency) presupposes security dilemma sensitivity: perceiving motives behind intentions and capabilities (Booth and Wheeler, 2008: 7). This applies equally to actors who desire to interact more profoundly and "to increase their voice and representation".

The increase in regional threats in the security environment after the Cold war is a showcase of the rising influence of cohesive regional groups in agreeing on norms that have in time facilitated more security. "A lesson here for emerging states that may yet have only poorly developed institutions, or for those that have traditionally relied on the politics of power, is that they cannot afford to ignore the potential of regionalism: and it is a lesson that has not been lost on the states of the former Soviet bloc" (Fawcett, 2004: 439). In a simplified form, regionalism provided a greater regional awareness and accommodated the growing need for involvement within an international environment more permissive to individual identities and purposes (also with the help of the "new" non-state regionalism). This certainly bears great relevance to the contemporary lack of security in cyberspace translating to national threats.

Nonetheless, it must be remembered that "regions and regionalism are what states and non-state actors make of them" (Fawcett, 2004: 434). Therefore, the question whether regional empowerment truly grows remains unanswered. "Clarifying and improving military doctrine on cyberwarfare, and by increasing the transparency of various cyberwarfare programs and units, states could better signal their intentions to potential adversaries and thus partially reduce the fear and uncertainty that exacerbate the security dilemma" (Rueter, 2011: 54). It remains to question whether transparency in responsibilities, even in military organisations, could leverage the impact of asymmetry inherent in cyberspace, the lack of attribution and number of stakeholders involved, to deliver such accommodating measures.

Obstacles to cooperation

"It is not unfair criticism to note that a number of institutions have never gone beyond the debate and discussion stage, and thus exist only as talking-shops" (Fawcett, 2004: 443). In the short-term, obvious impediments may come to mind, such as the lack of resources and capacities, be that in the legal, economic, or institutional field. The lack of resources may foster suspicion, rivalry and competition and make them persistent over cooperation. A separate but related impact is to be delivered also by the internal fragility of the state. Unstable cooperation, superficial effort and a dictate from a strong insider or outsider are among the impediments that regional organisations can encounter.

Also, the abuse of the regionalism capacity, rather than its reduction, becomes an inhibition. The abuse stems from the dominant state in the region. This notion carries weight because of the severe impact on the legitimacy of the regional institution once it can be argued that the regional project is an instrument of control. On the other hand, the same organization can be used (with limitations) also for containment of the powerful regional players (Fawcett, 2004: 444-445). The sovereignty that allows the states to state the willingness to further their interest must be carefully considered in this respect.

Major Concerns for Normative Regional Cooperation

Once regional cooperation overcomes or puts at hold the initial impediments, the states seek to cooperate on cybersecurity most often via information exchange, increasing law-enforcement cooperation processes and deliverables, and introducing and managing standards and requirements for secure conduct in cyberspace. The presence of such cooperation is in existence, as a rule, on an informal basis. Although formal agreements also occur, the scale at which they help to uphold the technical standards and security requirements, increase capacity building, promote online safety and reduce cybercrime does not influence the contemporary state of cybersecurity (Clark, Diffie and Sofaer, 2010: 185). Therefore, practical measures that plausibly ease the transcendence of broad norms stemming from the formal regional agreements and legal regimes will be introduced. These measures have been identified in the work of Clark, Diffie and Sofaer on the effectiveness of international cybersecurity agreements for advancing internationally agreed inter-alia objectives (2010: 195-201).

The following seven measures represent a set of concerns, the neglect of which would be detrimental in the context of a security dilemma. Thus, the focus will be strongly placed on the legitimization of the commitment among regional actors to reach a normative accommodation via regional legal regimes. The subsequent internalization of practices enhancing security in cyberspace relies utterly on the socialization delivered by the regional platform. Applying the measures regionally as opposed to internationally means to stress the shared concerns on cybersecurity related to regional legal, political, socio-economic, and technology-development particularities to "prompt justification for action and leave an extensive trail of communication among actors" transcending beyond this specific context (Finnemore and Sikkink, 1998: 892, 904, 907).

(i) Declaration of an agreement on limited specified objectives and norms of conduct for their achievement: This foremost measure defines the success of the agreement on a norm in question. The differences between activities regulated by the established legal regimes have a substantial effect on cooperation (Clark, Diffie and Sofaer, 2010: 185). As much as the designation of regulated activities stems from the number and sectorial origin of actors involved (civilian, military or private sector), there are more factors to consider. This includes the nature of threat faced by the stakeholders that, despite the shared local concerns, might not cover the particular strategic or operational perspective of an actor. Russia and China will respond differently to many of the broad threats that they share, as agreed on the 61st meeting of the Shanghai Cooperation Organization in 2008. While the Chinese use their cyber capabilities as an equalizer to delay and degrade a technologically superior opponent, the Russian strategic focus lies in psy-ops and the use of the content as information weapons (Arimatsu, 2012: 94, Ford, 2010: np).

Another such factor influencing legal regimes is the fluency of existing agreements that the security agreements could restrict. In other words, the cooperative agreements generally aim at minimum security standards as opposed to maximum security standards allowing for an uninterrupted run of the cooperation objectives. When the Chinese information security regulation in 2007 proposed mandatory security testing and certification for functions in technology such as routers, smart-cards, secure databases and operating systems sold commercially, the concerned industry groups including a European delegation to WTO and USTR (US Trade Representative) voiced their concern about such policy to pose a trade barrier to foreign companies. In 2009, Chinese officials agreed to limit the scope of the testing and certification requirements policy to governmental needs. USTR has also limited the scope of South Korean governmental agencies considering a mandatory adoption of an indigenous encryption standard as part of a large-scale government adoption of voice-over-Internet-Protocol systems. Otherwise, U.S. equipment and software suppliers would be forced to customize their products to comply with South Korean standards (US GAO-10-606, 2010: 35-36).

The expression of intentions and expectations are necessary for envisioning fundamental obligations, clarifying and setting standards but also for mitigating the "clashing cyber lexicons" (Kaminski, 2010:89). This will also help policy-makers realize the distinction between basic security that delivers obtainable and worthwhile cyber resilience and between complete cybersecurity (which is a myth) for developing instruments that are both technically correct and politically tolerable (Benitez and Healey, 2012: np).

(ii) Information-sharing on national legislation, national ICT security strategies and technologies, policies and best practices: The elementary importance of this measure resides in providing warnings of danger, remedies, and assistance with relief (see the effects of the lack of information-sharing in emergencies in the nuclear sector). A wider effort could overcome the reluctance to report in the private but also governmental sector and on the individual level, which would ease the implementation of remedies (Clark, Diffie and Sofaer, 2010: 196). Yet, concerns that information-sharing is not coordinated among the many stakeholders (and on the many levels) are pervasive. Much of those concerns reside within "political and national security considerations associated with sharing sensitive data" (US GAO-10-606, 2010: 35-36). In this sense, a barrier to effective international cooperation is imposed also by the lack of guidance on sharing the data. During the mitigation of the 2009 Confickr worm impact, "the

software company [running the mitigation] was unsure whether it was permitted to work directly with DNS providers located in countries the United States has labelled as state sponsors of terrorism." The interconnectedness of cyber threats merged with the lack of clear guidance to companies that are in addition disharmonized within a region undermines international efforts to mitigate cyber incidents (US GAO-10-606, 2010: 37).

An additional impediment to information-sharing and a more effective incident response is the sheer number of independent organizations involved in the response. An example of the disharmony is well present among the countries of the EU, despite the internal efforts to limit the differences (European Agency for Network and Information Security, 2014: np).[11] Companies outside of the EU, in this case a major US-based software manufacturer handling a 2009 cyber incident, seriously struggle to effectively communicate individually with each of the 27 member states of the EU. However, not only the regional harmonization but also a clear vision of cybersecurity trends, threats, and vulnerabilities in the region remains attributed to the "differences in data availability, consistency, reliability, and terminology" among the national-level CSIRTs (US GAO-10-606, 2010: 36).

(iii) Mandatory operational requirements and recommendations: The above-mentioned information-sharing problem also implies the importance of standardization of the processes during operations. Although the standards that regional concerts deliver for a safer conduct in cyberspace do not constitute law, they are expected to enable efficiency and cost-effectiveness in practice (meaning that they are not enforced but voluntary and compliance is easier).[12] Thus, cost-efficiency becomes a significant factor for cooperation and cooperative behaviour as such (Christensen, 1999: 61). The reason for its lack is in part to be attributed to the limits imposed on the influence of informal organizations and the adoption of "soft law" that by default applies cost-effective solutions. Such limitations could have far-reaching consequences on security in cyberspace. Take for example the slow progress on the migration from IPv4 to IPv6, the under-resourced developments on the DNS (the Domain Name System Security Extensions or DNSSEC), or the longwinded deployment of a more secure inter-region routing protocol (secure BGP) as envisioned by the IETF working with major equipment vendors.

An additional aspect to the standards is that they expand with growing numbers of their applicants. The Council of Europe Cybersecurity Convention (2001, Budapest) proves that the more actors participate in the legal regime, the stronger the community can enforce the agreed norms, making compliance natural instead of controversial, and non-compliance costly. Therefore, the Budapest Convention could generate deadlines for responding to requests, procedures concerning the seizure of data, production orders, expedited presentation, and disclosure, but also notification of attacks.[13] In the European community, controversial disclosure on security flaws and incidents residing in the possible legal consequences is slowly transforming into a common understanding of the necessity of the disclosure via the same legal means, yet founded in different mechanisms. Thus, using the existent mechanisms for mitigating a security dilemma among particular stakeholders, mechanisms that were formerly even possibly sustaining strategic ambiguity, with a switch in the normative objective proves by design far more effective for cooperation (Clark, Diffie and Sofaer, 2010: 188).

(iv) Commitment to act upon prohibited practices: The differences among individual national legal systems have long provided a clout for inaction if convenient (long- and short-term convenience

[11] For details on EU security policy and its criticism see Department of Business Innovation and Skills, "Call of Evidence for Proposed EU Directive on Network and Information Security: Summary of Responses" (GOV, UK, 2013: np).

[12] For different models of cost-effective cooperation (based on social network information centrality, trust-and-risk-based algorithms and resilient but trusted communities) and the benefits associated with their use, see (Hernandez-Ardieta, Suarez-Tangli and Taplador, 2013).

[13] For measures taken at the national level, see Chapter I (specifically Section 2 Article 18 for production order, Article 19 for search and seizure). For measures taken regarding international cooperation, see Chapter II (specifically section 1 Article 24 for extradition, Article 27 for provisions regarding mutual assistance requests).

should be noticed here) and been a safe harbour to strategic ambiguity. Without the sufficient technical capacity of the judiciaries and judicial systems and the consistent enforcement of existing norms, the cooperation on investigation and prosecution of cybersecurity incidents and breaches is less plausible not only according to adopted legislation but also informally. This legislative difference gains importance in the light of the broader context as it might reside within the lack of political or public support to enforce adopted laws (US GAO-10-606, 2010: 37). That the strategic ambiguity overcomes even the strongly embedded norms, shared by cross-sectorial stakeholders with common interests, resides within their material capabilities to impose punitive measures: "states and their militaries and security services will, even whilst pursuing denial strategies and improving defensive cybersecurity, be loath to abandon the search for effective punitive measures through which deterrence might be achieved. In turn, the norm of retaliatory punishment may prove to be a powerful deterrent in itself" (Stevens, 2012:165).

The commitment to act and enforce agreed norms is a measure that is necessary for escalating further commitment on a regional level and the tipping point for the transformation of non-compliance into compliance not only based on cost-effectiveness but also on socialization. The actual restraint on national actors and limit on their destabilizing conduct requires a full demonstration of sovereignty. In this respect, more important than harmonization alone is the interoperability of security systems that leads to meaningful MLATs (Mutual Legal Assistance Treaties) and criminal law practice (Clark, Diffie and Sofaer, 2010: 190).

(v) Law enforcement cooperation and mutual legal assistance: The cooperation on law enforcement is a measure entailing some of the most complex procedures and mechanisms legally, politically and operationally. Thousands of multi- and bilateral agreements in place with cyberspace as pervasive as ever for criminal activity is a good example of precisely how many difficulties this measure must overcome. It is necessary to involve key stakeholders, whether that is the telecom sector, the most interconnected country in the world or the state sustaining the most pervasive conditions for cybercrime. Moreover, the cooperative agreement must be clearly defined, as opposed to being vague, for the sake of consensus. The politico-legal intricacies take turn once the cooperation processes become politically misused (e.g. for extradition to undemocratic regimes that suppress political rights) or come to escalate to a unilateral action (in the form of a hack-back) under the pressure of time, the urgency of crime, and the impalpable evidence (Clark, Diffie and Sofaer, 2010: 196).

(vi) Capacity building for states requiring assistance: The difficulty of capacity building alongside with political maturity in less developed countries is well known. The fact that investment into the "gear" is futile if its operators cannot fully employ its potential has also been echoed by international organizations. Creating more equal development in human and technological capabilities has rather become the trend. Despite the strenuous challenge ahead, the need for capacity development in places that might most probably lack prohibitive measures on malicious activity is essential for these countries' performance under a legal regime.

(vii) Institutional enforcement measures: This measure stresses the relevance of an institutionally assigned authority. The number and form within which it takes place is a decision left to the members, yet this step is crucial for the success of the future legal arrangements. The authority holds hearings and collects evidence, decides upon financial obligations, memberships and voting rights but its most outstanding role is in imposing and enforcing remedies towards members who violate their commitments. The enhanced capacity of this authority could not only foster the acceptance of norms for a more resilient and secure cyberspace (Clark, Diffie and Sofaer, 2010: 201). Its effectiveness would have important distributional consequences that affect international agenda as well as organizational resource allocation (Haggard and Simons, 1987: 497, 516).

Cybersecurity Measures in Regional Organizations

The regional concerts with a cybersecurity agenda are not only "going global" because of the security issue they chose to address. The number of their member-base is in constant flux and their agenda subject to unprecedented change. However, the fact that cybersecurity emerges on agendas regionally is also a sign of great diversity in the individual perceptions of the ICTs and networks with respect to national security and political and economic deliverables. The following part of the article means to emphasize the diversity among the Shanghai Cooperation Organization (SCO), the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), and the Council of Europe (CoE) (Clark, Diffie and Sofaer, 2010: 197). The respective organizations introduce vastly different measures for reducing cyber threats and building resilience, which will be reviewed against the seven measures introduced above. The objective is a search for normative mitigation of the cybersecurity dilemma.

The Shanghai Cooperation Organization

The Shanghai Cooperation Organization emerged once Uzbekistan joined with the PRC, Russia, Kazakhstan, Tajikistan and Kyrgyzstan in 2001 and regional security was already at the top of the agenda. The organization prioritizes security and enhances the weight and prestige of Moscow and Beijing. The founding document is the Convention on Combating Terrorism, Separatism and Extremism, in which the two leaders share the approach on non-interference in internal affairs of sovereign countries and territorial integrity (Trenin, 2013: 5-7; Trenin, 2012: 30). This allows them to create a community rather than steer into a military alliance, also with regards to cybersecurity: "[t]hreats of a military-political, criminal or terrorist nature to information security constitute common challenges for all member states that need to be dealt with through prompt joint measures" (Shanghai Cooperation Orgnization, 2006: 2006-6-16).

The threat environment corresponds with the relatively high malware infection rates (not including Russia and China, whose rates are better) and a scattered Internet usage (Rashid, 2013: np). Of the seven FIRST certified cyber incident response teams in the region four are Chinese, two Russian and one belongs to Kazakhstan (Forum on Incident Response and Security Teams, 2014: np). The region counts one additional particularity and that is cyber censorship. What Russia, China, Tajikistan and Uzbekistan defend as "good conduct" for the Internet is believed to be the legalization of censorship. Of those, China and Uzbekistan have been coined "enemies of the Internet" and Russia and Kazakhstan labelled as "countries under surveillance" by Reporters Without Borders. Facebook-banning Tajikistan has been designated as "a country to watch" (Reporters Without Borders, 2012: 9). This leaves an impression of a region avoiding ambiguity in definition, yet absolutely sovereign and reluctant to pursue other than own security measures, regardless of external conditions.

Assessment of cooperative measures: most of the accounts identify the organization's scope on cybersecurity distinctive, yet too broad. However, integrity threats are preserved within, as the regime aims "for a more balanced international system" – with its substantial part entrenched in covering energy dependencies of the leading countries and the Central-Asian countries. Therefore, it is assumed that any measures taken towards cybersecurity (as envisioned by the parties) will not come into a conflict with other objectives (Trenin, 2013:9). Sharing the leadership has not facilitated closer cooperation in exchanging information and knowledge; on the contrary, Russia and the PRC expect one another to deal with outstanding issues internally. Despite that, the countries would seek each other's consent (as a mechanism of cooperation) to expand into the region to avoid opposition and confrontation (Trenin, 2012: 23, 26). Moreover, the region has agreed on using the already established regional organizations and the Regional Antiterrorist Structure to "strengthen international information security in all aspects" (Bishkek Declaration of the Shanghai Cooperation Organization, 2007: 2007-8-16).

Although information exchange is a foundation for cooperation and assistance in the organization's founding regulation, it is also designed to be "the initiative of the central competent

authority of a Party" (Shanghai Cooperation Organization, 2001: 2009-5-7).[14] Law enforcement is governed by the principles adopted during the Seventh Council Meeting of Heads of State that spell out the law enforcement procedures. According to the agreement, those are under all circumstances subject to national control over cyber systems and content (Clark, Diffie and Sofaer, 2010: 186). Organization-wise, the institution is rather competent in agreeing on and issuing a legally binding document at the annual meetings of the Heads of State Council that, in an extraordinary situation, is supported by a number of other bodies.[15] This institutional authority is greatly helpful in the delivery of normative documents. Yet, what the draft voluntary rules presented at the United Nations General Assembly point at is not so much the willingness to expand regional norms as the promulgation of a distinct and independent stand, fuelling the diversity that would need to be overcome (Arimatsu, 2012: 91-92).

The Asia-Pacific Economic Cooperation

The cooperative economic and trade forum is comprised of 21 countries located on the two sides of the Pacific.[16] This cooperation platform with two coasts holds countries suffering the most DDoS attacks worldwide like China, USA, Peru and Hong Kong. The Southeast Asian countries together with Peru and Chile also display some of the highest malware infection rates. Simultaneously, the inequality of broadband subscription in the regions is rampant. From the ban on freedom of speech and governmental regulation of the Internet perspective, China and Vietnam, yet also Australia, Russia, Malaysia, South Korea and Thailand employ heavy surveillance measures (Reporters Without Borders, 2012: np; Rashid, 2014: np). These conditions, however, give the organization a very different dynamic in comparison to the previous concert. The greater number of actors, despite it being a congregation of unlikely allies, delivers cohesiveness. A safe and trusted ICT environment is the group's foremost priority, right after growth and socio-economic development. The objective is to reach for better consumer protection but also a more trusted cyberspace via awareness, capacity-building and industry liaison (APEC TEL, 2010: np).

Assessment of cooperative measures: despite the astonishing differences on the national level, the cooperative organization has pursued the adoption of legal measures on cybersecurity with praiseworthy rigor. The ambition was not only to develop law but also to share information, issue security and technical guidelines and train and educate the "weakest links" among the parties for eliminating the inequality in capabilities in direct assistance projects to the Philippines, Indonesia and Vietnam in 2004. Together with the support of its robust awareness campaigns, the success came in the form of 13 of the 21 members adopting "relatively comprehensive cybersecurity laws", as described by the organization (UN GA Resolution 55/63; Downing, 2014).

Organization-wise, it is APEC's Telecommunication and Information Working Group (TEL) that supports security efforts associated with the information infrastructure of member countries through activities designed to strengthen effective incident response capabilities, develop information security guidelines, combat cybercrime, monitor security implications of emerging technologies, and foster international cooperation on cybersecurity. However, the TEL is rather than an authority an agent of collaboration with other international organizations, such as the ASEAN, the ITU, and the OECD but also

[14] See Article 6 (1), (3) and (7), Article 7 and Article 8 of *The Shanghai Convention on Combating Terrorism, Separatism and Extremism*.

[15] *The Shanghai Convention on Combating Terrorism, Separatism and Extremism* states that the Heads of Government Council meets annually to discuss a strategy and priority directions, important and pressing issues of cooperation and to adopt the annual budget. Meetings also run among the Speakers of Parliament, Secretaries of Security Councils, Foreign Ministers, Ministers of Defence, Emergency Relief, Economy, Transportation, Culture, Education, Healthcare, Heads of Law Enforcement Agencies, Supreme Courts, Courts of Arbitration, Prosecutors General and the Council of National Coordinators of SCO Member States. The two permanent bodies are the Secretariat in Beijing and the Regional Counter-Terrorism Structure in Tashkent.

[16] That includes the USA, Russia, China, Canada, Mexico, Peru, Chile, Japan, South Korea, then Hong-Kong, Tai Pei, Philippines, Thailand, Vietnam, Malaysia, Singapore, Indonesia, Brunei, Papua New Guinea, Australia, and New Zealand.

governmental actors (ministerial meetings) and private industries. The group stages international conferences across the region and provides the member economies with support for the development of response teams (in the public and private sectors). Such enhancement should serve the objective of respective national units joining in formal groups (Westby, 2004: 133-134).

The measures undertaken by the organization point at the value that is assigned to the online environment be it for individual empowerment or for economic growth. However, ICT infrastructure is crucial for the region and its sustaining is a key priority that dictates the forthcoming policies and agreements on conduct in cyberspace. The cooperation congress successfully implements the necessary measures for increasing the human and material capabilities of the region and for the mitigation of cyber threats and criminality, of which a longstanding practice and later a normative acceptance could emerge (Key APEC Documents 2013, 2013: 7, 62). However, it is speculative whether these practices will facilitate accommodation and when their growth will become intimidating.

The Association of Southeast Asian Nations

The 10 members of ASEAN have, according to the 2009-2015 Roadmap, resolved to combat transnational cybercrime, foster cooperation among their law enforcement agencies, and adopt cybercrime legislation. The agreement takes a more structural turn as it aims to enforce information infrastructure, expand and professionalize incident response teams and the training and education platform (US GAO-10-606, 2010: 35-36).[17] Coordination in the association took part in the telecom sector (for ICT resilience) and in home affairs. ASEAN's cybersecurity governing mechanisms include ministerial meetings and "Senior Official" meetings on transnational crime and on social welfare and development, a telecommunications regulators council, and a regional forum. The trade, services and liberalization that took place eased the facilitation of mutual legal agreements and cross-border procedures. In addition to that, ASEAN reaches out to its dialogue partners that include the EU (for law enforcement, judicial and prosecutorial cooperation), Japan, and China applauded by the community to be the "neutral broker" (Heinl, 2013:3).

Assessment of cooperative measures: while cybercrime was found on the agenda of the ASEAN Declaration on Transnational Crime as early as 2001, cooperation on information exchange, legal and law enforcement matters, training and capacity building, and extra regional cooperation has been identified in 2002, the Working Group on Cybercrime was established only in 2013 (under the voluntary lead of Singapore). The group focuses its mechanism mostly on connectivity maintenance (2010 Master Plan on ASEAN Connectivity: physical, institutional and people-to-people) and capacity building and development that includes people engagement and empowerment, trust building and collaboration among ASEAN CERTs (and their Incidents Drills: ACID) (ASEAN Secretariat, 2013: np).

The ambition to become a cybersecurity hub of excellence clearly drives ASEAN to operate with a plethora of institutional mechanisms. However, critics also warn that before this becomes reality, the disparate region must become more cohesive in enforcing the very same measures on its own governmental level. It is precisely the official public commitment that must rid itself of vagueness if it means for the region to succeed in the set goals (Heinl, 2013:2).

The Council of Europe

With 47 members and 11 observers to the council it comes as no surprise that the region encompasses three of the top victim locations for data breaches (US, Canada and the UK) as well as the top attacker locations (Romania, United States, Ukraine), and the top three malware hosting countries (US, Russia and Germany) (Trustwave, 2014: 10; Trustwave 2013: 7). Naturally, the democratic principles upon which the organization was founded now design the response to actions compromising confidentiality, integrity and availability of computer data and systems in a legal fashion. The legal

[17] The member base of the association includes Singapore, Malaysia, Myanmar, Indonesia, Vietnam, Lao PDR, Thailand, Philippines, Brunei, Cambodia.

measures adopted as domestic law focus also on the computer- and content-related offences and infringements of copyright and related rights. Nonetheless, it was expected that its membership will stand divided on the remedies that the Council proposed. Thus, the organization aimed at effective deterrence via a law enforcement treaty that would enable the collection of electronic evidence but also that defines and punishes criminal acts (Aslan, Celik and Dogrun, 2011: 185-6).

Assessment of cooperative measures: the Council empowers its members by granting them the authority to investigate, cooperate in enforcement through extradition and MLATs. Such measures will, however, work only if broadly standardized and within lies a possible weakness of its Convention on Cybercrime. The Convention itself is ambitious, as it covers vastly disparate areas of law enforcement, ranging from content restrictions (fraud or pornography) to limitations on hate speech, to misuse of device and system interference, where the domestic differences in individual domestic regimes are already irreconcilable (Clark, Diffie and Sofaer, 2010: 185-186; The Convention on Cybercrime, 2001: Article 1, Article 5and 6 and Article 9-12). Only one non-member has entered the Convention into force (the US), together with 30 members, leaving out the UK, Russia, Turkey, Poland and Sweden (Chrysopoulou, 2011: 13, 15-16).

Despite its meticulous structure and the implementation of a mechanism-easing compliance (24/7 contact network to immediately assist with cross-border investigation), the Convention, although a step in the right direction, has been labelled by its critics as "symbolic". That stands not only for the number of parties enforcing the Convention but mostly the lack of national clarity in its relationship with Internet service providers, which consequently impedes the investigation and opens the privacy issue (Marion, 2010: 704, 709).

Conclusion

Regional cooperation regimes possess the enhanced capacity to implement norms but the limits to convey the normative cooperation into practice so far have been identified in the practice of a number of regional organizations. Uncoordinated efforts (especially where interests overlap, SCO is an example, but also the number of actors active on the EU level) prevail over the internal and external coordination to reach global cybersecurity. Neither internal, nor external cost-effective measures to reach cybersecurity are applied accordingly. Although sufficient ambition as well as measures adopted might emerge in the future, those efforts would need to take into account the broad spectrum of stakeholders amenable to an open discussion of current practices. Despite these findings, regional cooperative regimes do not apply "a magical formula for transforming power politics and economic competition into cooperative internationalism… [rather] they are becoming viable means for creating norms and rules of interstate behaviour that are essential for establishing regional institutional architecture to manage collective economic and security issues, the process of which could possibly take at least a decade, if not decades" (Aggarwal and Koo, 2008: 31).

Miroslava Pavlíková

Introduction

In the contemporary world human rights violations in cyberspace are greatly discussed. The inventor of the World Wide Web has recently said that the democratic nature of the Internet is threatened by a *„growing tide of surveillance and censorship*" (Human Rights Watch 2013).

Nowadays, the phenomenon of internet regulation is linked to the Turkey protests, Arabian Spring and also to British anti-terrorism legislation establishing "control orders"[18] through the *Prevention of Terrorism Act 2005* (Alder 2007: 544 In.: Thiel 2009: 340). The case of Russian Internet regulation has been debated since 2010 but the first cases of information freedom violations have been noticeable since 2000 (with the start of Vladimir Putin´s governance). Since 2005 there has been a discussion about a new piece of controversial legislation in the Russian Federation, which should ensure national security against malicious Internet content such as extremism, drug propaganda, pornography etc. At the same time, the the most controversial pieces of regulation of the Russian government are usually those driven by political interest and officially justified as defending democracy. Kevin Rothrock, the editor of RuNet Echo, who interprets and also parodies the Russian Internet, emphasizes its uniqueness. He also stresses, that *"any real political alternative to the Kremlin is relegated to the periphery, where its public presence is limited to the internet*". As a result, Russian Internet becomes a platform for vibrant civic society expressions, which this is important to stress.

The main aim of this paper is to describe and analyse a Russian regulation regarding its cyberspace with a particular focus on human rights and freedom violations during the second half of 21st century and to consider its consequences in the cyber security context. Possible violations of human rights will also be inevitably discussed with a focus on regime type. In accordance with this we will operate with the concept of defence of democracy, which will be shortly theoretically explained. And finally, relevant legislation as well as specific cases, types and tools of regulation together with views of world organizations dealing with human rights will be introduced.

The main research questions are:

To what extent does a case of Internet regulation match the concept of defence of democracy?

Which tools of regulation could be considered as veritable examples of human rights violations?

Is it possible that cyber-attacks conducted by state sponsored groups will play a significant role in Internet regulation matters?

Defending Democracy

Democracy is frequently threatened by "*enemies of democracy*" like extremists, terrorists, or separatists. Defence measures (primarily legislative) often have negative effects on the rights and freedoms of citizens (in this context Internet regulation) (Thiel 2009: 1). "*The legitimacy and range of*

[18] „Control orders place restrictions on, inter alia, travel, use of the internet, and the use of telephones (Alder 2007:544 In.: Thiel 2009: 340).

self-defense is, therefore, a vital question of every democratic system" (Pfersmann 2004: 47 In.: Thiel 2009: 1).

In general, defending democracy or militant democracy[19] is a set of short-term (Cappocia 2000: 5) political strategies in modern western states, which should defend the system against „*forces that exploit the rights and guarantees of democracy in order to undermine its fundamental bases*" (Ibid.). At the same time, making democracy more militant increasingly modifies the structure from which it stems, so that a continuous extension of the domain of protection may amount to a decrease of the liberal heritage of constitutional democracy (Pfersman 2004: 53 In.: Thiel 2009: 103). Militant democracy is a term introduced by Karl Loewenstein (see Loewestein 1937a,b). His analytic design can be called "*binary*", because it poses a kind of dichotomy. Democracy can choose whether to defend itself or not; this is a choice between suicide and self-defence. According to many later theorists this approach is considered too narrow (Thiel 2009: 102).

In accordance with Thiel it is necessary to take a multidimensional approach to militancy. "The integration of the dimension of discourse enables the articulation of the relation between norms, political culture and the identification of the 'enemies' of democracy" (Thiel 2009: 103). Conditions of self-identification are considered, which helps to find a solution between the "liberty and security" dilemma.

We can define the *"enemies of democracy"* by the amount of risk, which for example terrorists could bring, by comparison to extremists, radicals or populists. The former two types are considerable for the case of the Russian Federation: anti-terrorist policies during the first decade of the 21st century and anti-extremist policies, which has been discussed for the last couple of years. Especially the latter – anti-extremist policies refer to new Internet regulation measures in the Russian Federation.

Carl Loewenstein (1938a,b) defines 14 main democracy defence measures. We will emphasize a few which have a potential linkage to Internet regulation. These are freedom of speech[20] restrictions, punishment of political crimes glorification, excessive political propaganda, or foreign anti-democratic propaganda.

Concepts of freedom of expression and information freedom are natural parts of democratic constitutions, including the Russian one. Article 29 of the Russian constitution proclaims freedom of speech and bans the violation of this freedom. Articles 23, 24 and 25 describe the right to privacy and data security, right to information, and privacy of the citizen's own communication. The words of Russian minister Shchegolev[21] at the London International Conference of Cyberspace in November 2011 as an official stance on manipulation with these rights: "(…)*this should be subject both to national legislation, and to counter-terrorism considerations"* (Giles 2012: 65).

Democracy and Russia

"*We are now living in a country that is anything but a democracy, it's a one man rule, and it is very clear that Putin's rule will not be stopped – by the ballot*," declared Gary Kasparov, one of the most famous opponents of Vladimir Putin.

[19] Interwar Czechoslovakia could be considered as an example of a typical militant democracy. The main challenge came from German ethnic parties, especially by DNP (German Nationalis Party) and the DNSAP (German National Socialist Worker's Party). These parties could be described as extremist, nationalist, secessionist, and anti-democratic. The government's reaction was to ban these formations and set up special laws limiting the functioning of extremist parties. With the rise of nationalist parties in Europe the Sudeten German Party started to be very successful. The measures had 3 pillars: a strong emphasis on rearmament, construction of military fortifications and equipping the state with legal means necessary to cope with internal and international emergencies, and „*the law on defence of the State*" (Cappocia 2001: 15-17).

[20] For the fundaments of the term, historical and philosophical context, see „*Freedom of Speech*" by Stanford Encyclopaedia of Philosophy 2012.

[21] It was reaction on UK Foreign Secretary William Hague who stated as a fundamental principle "*that cyberspace remains open to innovation and the free flow of ideas, information and expression*" (Giles 2012: 65).

"*Ironically, Russia probably experienced its highest level of democratic freedom in 1991, when it was still part of the Soviet Union*" (Rutland 2008: 3). Since the start of Vladimir Putin's rule in 2000 authoritarian means to retain power have been used. The established regime seeks to co-opt rather than eliminate its opposition. Although Russia possesses formal political rights[22], real power is concentrated around the executive branch. "Civil liberties[23] are even less secure" (Freedom House 2014).

According to the academic and also public discussion, the Russian Federation does not fit[24] into any democracy concept; practically it is the opposite of democracy (see Hloušek 2007). Permeation with Dahl's concept of polyarchy also could not be found in the case of the Russian Federation (where the need of "*understanding based on information*" is one of the conditions leading to democracy) (Mareš 2007: 251- 254). Regarding authoritative regimes, especially Linz's typology[25], there is also not (since 2001) a clear crossover (Balík 2007: 268-277). According to Freedom House (2015) the country is marked as *Not Free*. Since 2009 the Russian Federation is described as a "*consolidated authoritarian regime*" with a rating of *6,11*, where 1 represents the highest level of democratic progress and 7 the lowest. Up to the present day, the rating has slowly been declining. In 2013 it had already reached 6,21 and in 2014 6,29, while the level of independent media had remained at 6,25.

On the other hand, the biggest coherence is visible in the concept of a "*hybrid democracies*[26]", which are types that have stopped during their development process from an authoritative regime to a consolidated democracy[27] (Hloušek - Kopeček 2007: 285-295). To a wider extent *"illiberal democracy"* can be considered a form of hybrid democracy; this refers to regimes that combine the adult franchise and multiparty elections[28] with a failure to protect civil liberties (Gilbert 2011: 273). According to Gilbert (2011: 294) Russia was tending towards an illiberal hybrid regime (in the time period 1991-2009).

Regarding the political system we classify the Russian Federation as a super-presidential regime, which is officially constituted as semi-presidential.

Regulation of Internet Content: A Case Study of the Russian Federation

Agora, a Russian human rights initiative, differentiates between forms of Internet regulation, and deals with the case of Internet regulation in the Russian Federation. Agora (2012) considers instruments of regulation to be for example content regulation dictates, access denials, censorship, cyber-attacks, administrative pressure, but also criminal persecution, usage of violence, or violence with death consequences.

---

[22] See Constitution of Russian Federation.

[23] According to Dahl (1971) civil liberties (such as freedom of speech, assembly, and the right to alternative sources of information) provide the minimum conditions of procedural democracy by ensuring fair competition. „*Regimes that protect civil liberties provide a broad arena in which citizens can participate and thus have fair competition"* (Gilbert 2011: 285).

[24] "The boundary between democratic and nondemocratic is sometimes blurred and a broader range of variation in political systems lies beyond" (Diamond, Linz and Lipset 1988).

[25] Juan J. Linz distinguishes between totalitarian and authoritarian regimes, which both share anti-democracy.

[26] Gilbert (2011:271) uses this term for nondemocratic and non-authoritarian regimes. Otherwise, we can distinguish between more authors and variable approaches to the hybrid democracy concept. The first concepts were recognized by Zakaira 1997, Merkel 1999, or Diamond. Diamond operates with the „*electoral type*" which, in his opinion, is relevant to the contemporary regime of Russia (Hloušek, Kopeček 2007: 285-295).

[27] In accordance with Terry Lynn Karl (1995) the hybrid regime is a state establishment, which contains both democratic and authoritarian forms of rule. This duality – democratic and authoritarian – is the most dominant approach of conceptualizing „*hybrid regimes*". It especially refers to diminished subtypes of democracy as a response to the complexities of the third wave of democratization (see Huntington's The Third Wave (1991)).

[28] Although, this claim is disputable. It is not certain that Russian elections are free and without manipulation; a lot of human rights organizations stress the opposite.

Also, according to world human rights organizations (e.g. Freedom House, Amnesty International, Webindex) the described forms of actions are very often present in the Russian environment and its volume has increased in the last couple of years. Furthermore, cyber-attacks represent a new instrument of Internet regulation and offer a large scale of ways how to do it.

The introduced facts are useful examples for understanding the causality of the process of considering the case of Russian Internet regulation as well as its coherence with the concept of defence of democracy.

Figure 2 - Russian Internet regulation legislation

Legislation/law	**Description**
The Constitution of the Russian Federation	
Information Security Doctrine of the Russian Federation	"(…) goals, objectives, principles and basic guidelines for ensuring information security in the Russian Federation". Document primary focuses on the technical security of the cyberspace."
Criminal Code (N 63-ФЗ 1996) and its adjustments, especially an anti-extremist law	Crimes against government, defamations, propagandistic, racist or religiously exclusive content, and extremist expressions ("hate speech").
Federal Law of the Russian Federation (N 152-ФЗ 2003, N 126-FZ 2006, N 149-FZ 2006)	"On Personal Data", "About communication" and "On Information, Information Technology and Information Protection"
Draft Convention on International Information Security 2011	Document deals with the major threats to international peace and security in cyber space.
Conceptual Views on the Activity of the Armed Forces of the Russian Federation in Cyber Space 2011	Crisis management in cyberspace which should be maintained by Russian Armed Forces
Federal Law N 139-ФЗ (formerly known as № 436-ФЗ) and legislative measure 89417-6 2012	Measures for children's protection against malicious internet content
Anti-piracy Law 2013	Copyrights measures
Presidential decree N 31c 2013	Detection of cyber-attacks and protection against them
Legislative measure № 428884-6 (spring 2014)	Changes in the Federal Law "About information, information technologies and the information protection"; "The Bloggers Law"
Legislative measure № 553424-6 (July 2014)	Changes in federal laws dealing with personal data and telecommunication providers operating with it.

The table above introduces the development of Russian Internet regulation legislation since the establishment of the Federation. The following description and analyses emphasize events since 2010 and also consider the Ukraine crisis. Despite the fact that the Internet was not widespread in Russia and

bureaucratic interests in this field of society were not strong enough in the first decade, it is still important to mention this period because of its contextual consequences.

The 90's and the first half of the 21st century

As it was mentioned above, beside Jelzin's reforms there was also a conservative opposition with a strongly increasing influence. The struggle between Westernizers and conservative nationalists in contemporary Russia, according to Parland (2005: 3), is traced back to problems of Western modernization: Marxism and liberalism being products of the Enlightenment are confronted with conservative traditionalism. In 2005 this opposition wins the elections, Vladimir Putin takes office and dismantles the power balance, which has consequences in big companies' subordination to the Kremlin.

We recognize the end of independent television and partly also independent press when the media gets rid of undesirable journalists. One of the most known companies that are subordinate to the state is called Svyazinvest[29], a telecommunication provider, which owns nearly 90 % of telecommunication infrastructure. This fact evokes that state has much easier access to information and communication technologies of citizens (Budde 2014, Souleimanov 2006).

According to Souleimanov (2006), the enthusiasm[30] to continue in the strategic line of the Kremlin increased with terrorist attacks in 2002-2006 (Belslan, Dubrovka). Within the interest to provide security to citizens, human rights organizations and civil society have been limited. Considering the concept of defence of democracy, this fact is a paradox because these organizations are one of the main defending actors.

„*In the very end the Russians have less democracy, but their lives are definitely not safer*" (Souleimanov 2006).

The table above introduces important legislative measures, which deal with censorship issues and other new phenomena of cyberspace (e.g. the extremism laws from the 90's with a large range of implication). In 2006 the legislative dealing with ICT usage and cyberspace comes in force. This federal law has been changed many times with new controversial legislative measures.

In 2005 in accordance with Freedom House (2014a) Russia has returned to the category „Not Free" primarily because of Vladimir Putin's power culmination, repressions in the media sphere and polarization of the legal system.

Internet popularity increased during the first decade of the 21st century and the first blogosphere appeared. These bloggers and Internet activists (opposition mainly) have been persecuted ever more frequently, extrajudicial processes by the Federal Security Service (FSB) appear as well as cyber-attacks on their web pages. At the end of 2010 the initiative Opennet, which records regulation on the internet, published an analysis focusing on the Russian case in which the selective filtration of social and political content and low transparency and consistency is evident (Opennet Initiative 2010, Freedom House 2014). Otherwise, Russia had relatively lax internet laws during this period. New, stricter legislature has been progressively forming in recent years. In accordance with this, Vladimir Putin has started to brand the Internet as a „CIA project" (BBC 2014a "The Bloggers Law").

The second decade of the 21st century

In accordance with the Agora Human Rights Association there has been a rapidly growing amount of internet users in the Russian Federation after 2010. In 2011 it was 40.7 million (49 %), while it had reached 46.8 million in 2012. The government strongly supported technology development especially through the Svyazinvest/Rossvyaz (ISP), which helped thanks to its low prices. In contrast to this there were internet access restrictions, which were accompanied by restriction measures for providers, all appointed by president Medvedev. Although there have not been official direct restrictions, Freedom

[29]Iinternet Service Providers (ISP) included in Svyazlvest are e.g. Central Telecommunication Company, North-West Tele-com, VolgaTelecom, Southern Telecom, Uralsvyazinform, Sibirtelecom, Dalsvyaz, or Central Telegraph (Budde 2014, Souleimanov 2006).

[30] Contrary to this, we could mention Vladimir Putin's stance from 2002 when he had refused to sign the Duma's legislative measure regulating the media.

House (2014b) stresses the unfair competitiveness, corruption, and other measures corresponding with internet regulation after 2010.

Internet regulation in 2011 and 2012

The following list is a result of Agora data acquisition and research and it focuses on internet regulation in the Russian Federation in 2011 and 2012. In its analysis the high increase of freedom violations by Russian authorities mentioned below has been emphasized (Digital Trends 2013). According to the report, the legislative measures dealing with internet regulation in 2012 have caused something called *"the web of sovereignty"*, i.e. Russia is moving in the same direction as China or Arabian states. In 2012 we recognize 1197 cases of internet regulation (in contrast to 2011 when it was 500) (Agora 2012).

Figure 3 - Forms of Internet Regulation in RF

Forms of Internet Regulation	**2012**	**2011**
Violence resulting in death	0	1
Use of violence	3	10
Internet regulation suggestions	49	5
Criminal persecution	103	38
Administrative pressure	208	173
Access denial	609	231
Censorship	124	No records
Cyber attacks	47	31
Others	54	11
Total	**1197**	**500**

State-controlled providers in the Russian Federation

The presidential decree signed by Dmitrij Medvedev ensured a fusion of the original Svyazlnvest and the RosTelekom, which in fact means that the Russian government has gained nearly absolute control of the internet (Freedom House 2014). Therefore, the big issue lies in the relation between state control of users' data and the companies' linkage to the state in such a huge range. Since the year 2000, the Russian providers have been working under the *"system for investigative measures",* which, in fact, allows FSB and the police access to internet traffic. The system works on the same principle as Carnivore/DCS1000, which has been used by the FBI for information analysis of the web. With this software FSB can follow user's transactions, e-mail communication, or web searches in real time (Freedom House 2014, Opennnet initiative 2010).

Internet content is being changed and blocked very often because of ISP[31]. The blocked content is often marked as extremist and blocking it is the effective way of dealing with it. But the process of identification of extremist materials is not always transparent and providers are often repressed even if their pages are not mentioned on the blacklist of the Ministry of Justice. A lot of terrorist, extremist and separatist[32] groups' pages were banned but it was discovered that a lot of pages without any notable extremist[33] content we also on the list. We are witnesses of a massive exodus of opposition web pages to providers abroad. Since 2011, well-known domains like ".rf" or ".ru" could be blocked[34] in accordance with a new executive instrument (Ibid.).

Federal Law N 139-ФЗ and legislative measure 89417-6 2012 concerning children's protection against malicious internet content

A largely discussed federal law about children's safety on the internet is actually a correction of a few former laws.

After this measure came into force (the exact translation is "Children's protection law against information which is harmful to their health and self-development")[35] and very soon it started to be called a censorship tool instead of an instrument of good intentions. Besides its official focus against pornography material and suicide promotion it has also been used for political purposes (Gaudarsvenaja Duna 2013, Sovjet pri prezidente RF 2013, Digital Trends 2013, Freedom House 2014).

In June 2014 the measure "*o chiernych spiskach*[36]" (from the original черных списках; translated to English as "blacklists") was adopted. It establishes[37] the blacklists of malicious web pages (BBC Russia 2012). The blacklist[38] has been defended by the Kremlin as an instrument ensuring healthy children's development, which is aimed by the prohibition of malicious internet content. In combination with the anti-extremist law mentioned above, these measures are practically applicable to everything. Besides domestic and foreign activists, parts of the opposition are also against this new legislation, moreover, they feel unsecure because it may be used against them. The Russian minister Nikoforov clearly refused these accusations (Ihned 2013b). At the end of 2012 the Russian Pirate party stated that 96 % of pages[39] on the blacklist are there without any justification (RIA Novosti 2012).

On the other hand, globally popular providers adopted a more conciliatory position with the new measures because naturally their potential presence on the blacklist is not very favourable[40]. In the new measures, steps against drug propaganda on the internet are also emphasized. Therefore, the Federal Drug

---

[31] Internet service provider.

[32] KavkazCenter.com, Tawba.info, Limonka.nbp-info.ru (…) (Freedom House 2014).

[33] Freedom House (2014) mentions for example the Jehovah Witness web pages.

[34] According to the United Nations Human Rights Council, web pages in Russia without malicious content are also regulated because of IP address connections. These are also present during wider blockades when domains are closed. This connection could slow web requests and increase insecurity of user's data. "*Censorship or an electronic curtain in the Russian internet environment should be stopped, because it causes human rights violations or damages civic society or national economy"* (RIA Novosti 2012, RIA Novosti 2013b).

[35] „*The law should primarily deal with our children's protection against narcotics, paedophiles, and promotion of suicides*" (Pirate party 2014). The Pirate Party considers that this kind of legislature is practically useless (as an example the party mentions graphics which show the decreasing popularity of children's pornography in the last few years as well as little intentions in drug or suicide information internet searching (Ibid.)

[36] Right after the "blacklists" came into force the suggestion for sanctions against anonymous authors and law disobediences from „United Russia" had appeared (Agora 2012).

[37] Two weeks later there were 180 web pages on the blacklist. Some personal pages on social networks, as for example Vkontakte.ru, have become unavailable, too (Ihned 2013).

[38]The official title is „*The unified register of domain addresses and web sites in the information and the telecommunication network Internet whose disclosure is prohibited in the Russian Federation*".

[39] The Pirate Party-led web page rublacklist.net called RosKomSvoboda informs about censored or blocked pages.

[40] These examples of „self-censorship" are also linked to post-deleting on internet forums (Sidorenko 2011).

Control Service also has executive power in the process of identifying malicious internet content. But the most powerful body in this decision-making process is a special agency called Roskomnadzor (Ihned 2013). Roskomnadzor operates the web page http://rkn.gov.ru where it is also possible to add anonymous suggestions for regulation. The process of this announcement is an elementary procedure. The main issue is the process of deciding who should be blocked because this execution does not need any legislative cohesion. The prime minister is the one who decides about the leadership of the agency and this process in not described as transparent (Freedom House 2014b).

Antipiracy law

The law[41] came into force after a long preparative process in August 2013 and it was followed by protests of internet users and companies (10 000 citizens signed the petition within two months). In regard to legislation measures mentioned above and the anti-extremist law tools this law was largely criticized especially because of its potential for unjustified implementation (RIA Novosti 2013a). The state has the power to shut down websites without a court order if there is suspicion of using copyrighted materials illegally (Freedom House 2014).

Legislative measure № 428884-6 „The Bloggers Law" and Legislative measure № 553424-6

The new legislative measure that brings changes into the main Federal law dealing with information has been named the „Bloggers' Law". The law, officially signed by Putin, requires popular internet writers to follow rules normally reserved for larger media. Bloggers with more than 3000 readers are required to register. Interaction of Roskomnadzor with this law can be accompanied by the removal of information, inaccurate data, or harmful posts (The Verge 2014).

The main issue lies in the most basic element of blogging: anonymous publishing. Political activists and dissidents could now be easily detected and the application of other internet restricting laws has followed. Popular bloggers are already looking for a way to „cheat" the feature that counts page visits (The Verge 2014, BBC 2014a) On the other hand, the law consists of more anti-blogger provisions. The law prohibits them to register as a media outlet but they are required to certify the factuality of the information on their blogs. It also bans the publication of citizens' locations, domicile, personal, and family lives. This kind of information publication could deal with official's illegal property, which was discussed for example by the internet activist Alexand Navalny (The Moscow Times 2014).

Another measure dealing with users' anonymity dictates that social networks must maintain six months of data on its users. Moreover, the data must be stored on servers based on Russian territory, so authorities can gain access to the data easily (BBC 2014a). In fact, it means that social network owners along with e-mail providers are required to store information about their users, posts, and communication. Some internet experts are afraid this can lead to a total closure of social networks such as Facebook, Twitter, or YouTube (BBC 2014a, The Moscow Times 2014).

Cyber Attacks

"Russia and cyber attacks" is a largely discussed phenomenon with a widespread scale of consequences. But is it possible to regulate internet content by this specific tool?

The amount of cyber attacks has increased during the analysed time period. Especially there were DDoS attacks and attacks with a phishing character. These types of actions have been investigated only when the victim had been the state apparatus (for example the company Аэрофлот (Aeroflót) in 2010, or the president's and government's web pages in 2012) (Agora 2012). During the Duma elections in 2011 a number of running parties' pages were attacked by a series of cyber-attacks with botnets usage. Some organizations and voters accuse crime groups sponsored by the state. Most of the attacked pages had a

[41] In the public sphere it is known as the "Russian SOPA" or "the anti-internet law".

particular connection to the opposition parties and media, but also to the "pro-Kremlin" ones (BBC 2011, Agora 2012, Roberts 2011). [42]

The presidential decree dealing with the recent cyber-attacks law came into force at the start of 2013. It is still a question to what extent all the attacks will be prosecuted, not only those linked to the Kremlin.

Nashi and *Molodaya Gvardiya* have been discussed as potential Russian hacker groups with a linkage to the Kremlin. They have also been considered as the responsible ones for cyber-attacks in Estonia in 2007. Some people accuse them that they have been played for producing Putin-supporting internet content and cyber-attacks against dissent. Types of attacks the groups use are said to be DDoS and phishing activities.

They have also been confronted with an anti-Kremlin group widespread all over the world: *The Anonymous*. They are well known for their attacks on the pro-Kremlin hacker groups, especially on their mailboxes or just young profiling Kremlin groups (e.g. Federal Youth Agency). The rivals steal the other's e-mail correspondence, which is respectively different in its character. The anti-Kremlins try to prove criminal and[43] anti-democracy activities and the Kremlin-supporters focus on personal data[44].

An e-mail conversation between the former Nashi group leader Vasily Yakemenko and the spokeswoman of the Russian Youth Committee Poputchik has been stolen and shows preparation of unlawful actions on the internet. Several of their e-mails include a price list for pro-Putin bloggers and commenters, indicating that some are paid[45] as much as 600,000 roubles for leaving hundreds of comments under negative internet articles[46]. In accordance with e-mails, Nashi manipulate Youtube view counts and ratings calling on paid activists to „dislike" anti-regime videos (The Guardian 2012, ITAR-TASS 2014).

Thus, we are practically facing a cyber-struggle between two ideologically different groups, where the first is committing cyber-attacks for regime propaganda and the second is attacking back to prove these activities.

Conclusion and Analysis of Internet Regulation in the Russian Federation

According to Freedom House the "Freedom on the net" is marked "Partly free"; this value has not changed much in the two-year period. Political censorship was not registered, but the persecution of internet activists was as well as restrictions of press freedoms (Freedom House 2012, 2013). Webindex, the website monitoring internet freedom (see its founder Tim Bernes-Lee above) marks the Russian Federation with a value of 47.1 (100 max), relevant content reaches only 60.2, and openness and freedom 26.5 (Web Index 2013, Human Rights Watch 2013).

[42] For a list of attacked pages see http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/

[43] See the page http://slivmail.com/ with published e-mail communication which also consists of communication between persons linked to Nashi as for example Krisitina Poputchic and Artur Omarov.

[44] For example against the activist Alexandr Navalnyij. He is one of Putin's biggest media opponents and a symbol of the fight against internet regulation. His activity has been largely limited in the last 2 years (cyber-attacks on his web page, blockade of his page *navalny.livejournal.com*, home imprisonment, and prohibition of access to the internet since 5.4.2014). But also other subjects that share or cite Navalnij face problems (radio Echo of Moscow). Since he cannot express his thoughts on the internet, his family and supporters continue with his accounts (e.g. https://twitter.com/Navalny_En). Navalnyij is also one of the persons on the *Traitor.net*; a list of traitors of the Russian Federation, especially because of their negative stance toward Russia annexing Crimea.

[45] One of these e-mails suggests that the group planned to spend a great amount of money to buy a series of articles in two popular Russian tabloids *Mosovsky Komsomolets* and *Komsomolkaya Pravda*.

[46] There can also be found anti-opposition pages with the possibility of active involvement of readers. The web page predatel.net allows them to insert persons with citations that criticize the establishment of the state.

The following analysis will answer the research questions, which serve also to summarize the whole text.

Considering the concept of defence of democracy and its application on Russian internet regulation, we will emphasize a few analytical points. The first is a definition of democracy enemies. The introduction of legislation has shown that by democracy enemies extremist groups, political radicals, populists, or terrorists (in earlier periods) are meant. It is understandable that after the terrorist attacks in Dubrovka or Beslan the Russian Federation set relevant measures for the defence of democracy, but there are also cases when there was not a clear focus on indices of terrorism, extremism etc. Another point discuses the rights protected by regulation and aims that were reached. One of the largely discussed pieces of legislation – the "*children's protection law*" has been stressed as ineffective with discrepant purpose many times. In accordance with human rights organizations and other initiatives, 96 % of webpages are on the blacklist without justification. We can also mention the closing of IP addresses, when also harmless websites have been shut down. Moreover, these unjustified restrictions could be considered as human rights restrictions itself.

The third analytical dimension focuses on executive power relevance – bodies which decide about regulation. As we could see, in the Russian Federation some bodies are non-transparent and sometimes operate without the valid legislature. Therefore, the relevance is very disputable.

Next, how do international human rights organizations react to Russian internet regulation? As we emphasized above, a number of initiatives do not support this kind of "defence of democracy". Thus, it is inevitable to consider Russian internet regulation in the democracy defence prism as quite doubtful.

Finally, let's discuss the character and type of internet regulation. These are primary measures based on the "blacklisting" represented by Roskomnadzor. There are also variable ways to suggest a subject of restriction and they cover active participation of civilians. Secondary ways of regulation, which were presented by Agora above, are present as well. The understood measures are usage of violence, criminal persecution, access denials, and also cyber-attacks. A number of emphasized cases could be considered as human rights violations, as it is also largely stressed by an amount of human rights initiatives. Usage of cyber-attacks as tool of regulation may play a significant role in the future. In the Russian Federation there are cases when state-sponsored groups lead systematic cyber-attacks against opponents. Groups like Nashi could become new, fast, effective, and non-transparent forces, which authoritative regimes can use as a financially inexpensive executive power of its unpopular and unjustified measures.

Regulation of the Russian internet is a real thing. Internet is regulated in many parts of the world; in some cases it is for democracy protection, in others for regime protection. This is also the case of the Russian Federation, which is genuine in measures and tools that are used. The mentioned cases are of course alarming, but it is necessary to keep in mind that Russian cultural patterns play a big role in the acceptance of the tools and measures. The character of the Russians could be incomprehensible for the West and could therefore call for radical solutions. And as it has happened many times in our modern history, it also wouldn't be too strange if the Russians would see these kinds of regulations as quite legitimate.

A Sociological Approach to Cyberspace Conceptualization and Implications for International Security[1]

Nikola Schmidt

Introduction

The reason to write this chapter emerged due to a strong critical conviction about the perspective scholars have used to approach cyberspace in order to assess its implications in international security. A lot of papers have been published scaring the world community with new catastrophic cyber threats. The securitization discourse started over two decades ago with a paper by John Arquilla and David Ronfeldt called Cyber war is coming! (Arquilla and Ronfeldt 1993). However, it has not changed significantly to the present day. White House employees publish books (Clarke and Knake 2010) with alarming cyber implications close to an Armageddon. Those conclusions are very questionable, as they are not based on the technical reality of cyberspace and its capability to be appropriately updated or shaped to meet security needs, but understand all the possibilities in and vulnerabilities of cyberspace as a security threat.[2] The core of this securitization discourse usually takes the reality of a kinetic war and applies it to cyberspace that is treated as a new warring domain (US-DoD 2011), in which cyber weapons are treated similarly as conventional weapons.

Cyberspace as a term was firstly used in the science fiction book written by William Gibson Neuromancer (Gibson 1984). It was used to define cyberspace as "a consensual hallucination." Fifteen years later, after the Arpanet, a predecessor of the Internet, was launched, cyberspace simply did not exist in the minds of policy makers. Later, in 2011, the US administration defined cyberspace as the fifth domain of warfare by announcing its defence strategy for operating in cyberspace. In 2013 a group of worldly recognized lawyers published a book called Tallinn Manual of International Law Applicable to Cyberwarfare (CCDCOE 2013). Although scholars usually treat cyberspace as a borderless space,[3] the manual in fact granted cyberspace borders by assuming states a right to exercise their jurisdiction over cyber infrastructure situated within their territory. All those mentioned milestones somehow construe the way we understand this virtual world or phenomena of cyberspace and how we interact with it and how it interacts with us.

However, treating cyberspace as a warring domain is not a problem at all, the problem lies in understanding cyberspace dynamics in the same way as the physical space. Scholars that commit such an epistemological mistake simplify the problem without trying to develop a theoretical foundation that would offer an appropriate reflection of cyberspace and related emerging threats. This uncritical approach leads to warnings such as "cyber war is inevitable, unless we build security in" (McGraw 2013), arguing that defensive measures have to be implemented in the systems by design. In fact, IT systems will be vulnerable forever due to their rising complexity; such a point of defendable systems has passed and is now unreachable. The explanation lies in the fact that systems are not becoming simpler, but more complex, interconnected and sophisticated and designing systems without vulnerabilities is not possible; thus the number of vulnerabilities will rise. The EU Cyber Security Strategy understands the problem precisely and calls for systems' resilience (EU 2013) rather than defensive measures. Such an argument does not oppose the idea of developing better security in design of course (e.g. better cryptography methods). However, the long-term strategy in securing cyberspace has to look at the problem from a much wider perspective. Technology is not the only unit that cyberspace is comprised of; technology

[1] This article was supported by the grant project no. 538213 funded from the Grant Agency of Charles University.

[2] This is a common approach of policy makers criticized by a broad spectrum of academics. See for example .

[3] For example, an article by Giancarlo Grasso treats cyberspace as a borderless space when discussing the results of infrastructure infection or attack (Grasso 2009).

itself intensively contributes to the way we use it. Hence, it is about the way it is used, and in the end about a completely new shape of conflict that waits to be conceptualized.

Every newly developed significant technology influenced society throughout history. It changed habits, routines and the way we see and solve problems. Invention of the Internet, and thus the emergence of cyberspace, has changed society immensely and caused an unprecedented shock to its structure. The emotional reaction of the world community to the connection of a personal computer to the Internet in the end of the 1990's was so significant that we simply forgot how extraordinarily our lives – in the sense of day-to-day activities and consequent dependency – have changed during the last two decades. We have adapted to a new environment and communication methods. Our lives are closed in frameworks of habits and routines that create social structures; which have changed accordingly. However, the invention of cyberspace created a completely new space for our habits and routines, and in the end for a new way to reach our goals. Cyberspace does not allow physical movement, hence kinetic conflict is not possible in cyberspace, but it is possible to influence physical systems using cyberspace that operate out of it. Cyberspace can be used to allow or trigger a kinetic attack or additionally to produce another kind of conflict with the vast novelties that cyberspace brings. The current state of knowledge does not lead to strategies that would solve an emerging security problem; it applies knowledge from different spheres of human experience that cannot be applied to cyberspace so easily.

This chapter has the ambition to offer a new perspective of cyberspace as a non-physical but cognitive (constructed) space that has direct implications to international security in an unprecedented way, but one that is sharply different that the current military-oriented securitization wave of cyberspace addresses. It does not omit commonly accentuated cyber conflicts but analyses the cognitive ones in a theoretical perspective with its factual implications to international security. The classical sociological approach in constructivism is used to conceptualize the so-called fourth layer of cyberspace (see below) that would significantly influence our habits, social structures and decision-making.

There are two pivotal objectives in this article. First, to lay down a conceptual framework on which the cognitive layer of cyberspace should be analysed and to propose this framework in a way that can be simply applied to selected events in cyberspace. Secondly, to use this framework as a methodological approach in uncovering institutionalization processes in cyberspace through a constructivist lens with two specific impacts: an erosion of the state as a traditional actor, and as a dominant actor over its physical territory.

Cyberspace Definitions and Characteristics Discussed Today

Security-oriented papers tend to define cyberspace from a technical perspective only. These definitions are a problem themselves because of their prevalently technical orientation that devalues the analysis in the realm of incomplete definition. For example, Dorothy Denning delivered the following definition in the past: *"Cyberspace is the information space consisting of the sum total of all computer networks"* (Denning 1998)*;* she understands cyberspace as a mere sum of technological units. Walter Gary Sharp puts the World Wide Web on the same level: *"Cyberspace… [is the] environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web"* (Sharp 1999).

Those definitions are out-dated. Some new ones meet expectations of cognitive add-ons such as the one introduced by Kuehl: *"Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures"* (Kuehl 2009). The core cognitive added principle is in the phrase *"is framed by the use"*. Interaction between a human being and technology has been added even though it has not been thoroughly theorized. The phrase exactly says that the shape of cyberspace *is framed by the use* of it so the unit and the structure are interdependent. However, the joint publication of the US Army concerned with Information Operations (IOs) (Scaparrotti 2012), from which the above-mentioned definition is abstracted, divides IOs into three interlinked dimensions: systems that provide

connectivity; *content* or information that can be sent or received without delay from or to anywhere in global cyberspace, and human *cognition* representing the way humans react and make decisions. This perspective will help us in the following approach to cyberspace conceptualization.

Martin Libicki, the world-recognized RAND scholar, introduced an idea of a four-layer cyberspace. In Libicki's meaning, the first layer consists of the physical infrastructure of hardware, cables, routers, satellites on orbit etc.; the second syntactic layer consists of principles on which the physical systems work, such as communication protocols; the third semantic layer consists of data flowing in the systems or saved on hard drives; and the fourth layer is pragmatic (cognitive) which would be "hard to define" quoting Libicki (Libicki 2007, 8). Then he analyses and assesses the means needed to conquer each layer. The first may be conquered easily by taking over or by destroying the infrastructure; the second can be conquered by influencing the behaviour of all the related systems, by injecting them with malware or by any other means that influences their operation; the conquest method of the third layer, in Libicki's perspective, entails manipulation of information or content of cyberspace. However, Libicki neither thoroughly theorizes nor evaluates the possibility to conquer the fourth, pragmatic (cognitive), layer. The lack of the fourth level theorization is not something that Libicki simply missed, but he did not give the problem deep enough attention (Betz and Stevens 2011); maybe due to its alleged overlap with the semantic layer.

Treating cyberspace as another domain along with land, sea, air and space as stipulated in the US Department of Defense Strategy for Operating in Cyberspace (US-DoD 2011) cannot be understood as a definition of cyberspace (by its equation to other domains). The DoD encourages the US security community with Pentagon in the lead to *"organize, train, and equip"* with objective to *"take full advantage of cyberspace's potential."* The mystification between definitions or knowledge that may be used as an epistemological approach to cyberspace and the governmental appeal to *"organize, train and equip"* is a common mistake found in the literature regarding cyberspace. The domain simply does not exist in the same form as all the other four domains of land, sea, air and space. All those four domains ontologically exist and a human is challenged to gain the strategic advantage by adopting a particular technology, knowledge or abilities. We need wheels to ride on land, hull to sail at sea, wings to fly in the air and thrusters to manoeuvre in outer space. However, one apparent characteristic changes everything. Cyber space as the fifth domain is a man-made domain and the tools needed to operate in it may change significantly and immediately. There has been an immense debate over the novelties of cyberspace, but not one (to the author's best knowledge) conceptual framework that would serve such strategic purposes on a cognitive layer.

Cyberspace has already received several particular characteristics that should be taken into consideration. The characteristics were well-listed e.g. by Choucri in her book Cyber Politics and International Relations (Choucri 2012). Those include: *the attribution problem* – the problem that complicates unveiling the attacker; *temporality* – time loses its sense and temporality switches to near instantaneity; *physicality* – the exact geographic location transcends; *permeation* – boundaries blur and thus the impact of jurisdiction is limited; *accountability* – as the jurisdiction and attribution are limited the accountability is indistinct; *fluidity* – continuous shifts and reconfigurations (Choucri 2012, 4). Each of the above characteristics is usually debated in isolation. However, even together they cannot perfectly grasp cyberspace. As said, it implies following. When an international team of experts writes a book about international law applicable to cyber warfare they omit the *physicality* of cyberspace at least. The trap for objectivists and positivists lies exactly in the limits of their reflection on measurable units (positivists) or in conventional frameworks (international lawyers). Fluidity is hard to grab, hard to explicate, hard to comprehend, but it does not mean that such an evident characteristic can be omitted. It should be theorized and implemented in cyberspace conceptualization before developing new strategies or norms.

Albert-László Barabási has developed an inspiring theory of networking more than a decade ago (Barabási 2002). He understands a broad meaning of a network. It is not only a network of computers, but it may be a network of mycelium or social network as well. Network in his meaning consists simply of nodes and connections between them. He spends a large part of his book on the analysis of its dynamics.

The important finding in his thoughts is the natural tendency of each network to create important nodes – centres – by making preferences. In the social network of humans these nodes are created by important persons; persons preferred by others as the others understand the selected persons to be important, valuable and important in their own social network.

However, human habits create centres as well by preferring specific services and ignoring their alternatives. They are gradually preferred due to routines that, in our minds, secure the fulfilment of desired goals. If we have experienced achieving a goal by a particular means we tend to avoid alternatives even though they may lead to the goal using a shorter path. It shapes the cognitive layer and defines centres when we prefer Google, Facebook or other services. Cyberspace, thus, is not just a mess of cables around the world, but it is also a space of interactions that reflect our habits. If challenged, it may sink society into Durkheim's *anomie*. Hence, it is not only about infrastructure, systems, content, but also about *the way we* – repetitively – *use it* and thus shape it continuously. Development of an appropriate conceptual framework and consequent strategy for such a space is a challenging but essential task. If states are tasked to *"organize, train and equip"* in this domain, the above-mentioned characteristics are essential.

Conceptual Framework of a Cyberspace Cognitive Layer

The development of a theory dealing with a social, security or international relations problem, or the clarification of measurable processes in natural sciences have the same importance in any piece of academic work – to develop a theoretical lens that would serve as a better understanding for anything *out there*. Laying down a conceptual framework would appropriately serve for the understanding of the dynamics of the cognitive layer. That is the reason why we use the term *framework conceptualization* rather than *cyberspace theorization*, but as such it has to be based on a general theory in order to be comprehensible. Therefore, the application of a general theory of a specific epistemological approach to new ontological problems would provide us with a different perspective on cyberspace and would serve for better policy development.

Laying Down a Constructivist Perspective

It is valuable to use the constructivist approach (key concepts are in italics), in its basic version represented by Berger and Luckmann (Berger and Luckmann 1966), but also in its second wave represented by Bruno Latour (Latour 1996). The former approach is a well-known pioneer constructivist piece of work and a classic in broad social science application, whereas Latour came up with an idea that also technology with its automated or pre-programmed behaviour constructs our reality (Alvesson and Sköldberg 2009, 31).

Berger and Luckmann's work is valuable in its analysis of everyday life. The core lies in an inter-subjectively constructed reality. *Habitualization* is a process of following our *habits* and *routines* we adopted during *socialization*; during a process of forming such habits compatible with society's expectations. Let's define habits for further purposes as a process in which we adopt specific behaviour to achieve *intended* results with higher probability, and routine as a process in which we do the same *unintentionally*. If we add a certain actor to such a *typification* of activities we construct an *institution*. Hence, any kind of behaviour that is recursively on-going by certain actors creates an institution. And institutions have specific dynamics with an impact on the initial and other actors and their preferences in the adoption of new habits. This backward effect is *social control*, whether intended or unintended. Some activities we conduct are somehow controlled by being *anticipated or expected behaviour*; that is the unintended social control that constructs a culture of behaviour. Cultures differ as the development of such social control has developed on anticipative reactions of other actors. If some important actors were unsatisfied, they would have strong intention to change such a social culture. Priests were usually important persons in the middle ages and earlier, because they represented a pattern of *admirable behaviour*. On the other hand, it is common knowledge that those people bend reality to let others fulfil their own interests; powerful people generally tend to do the same, influence actors around them to

achieve an intended result – an objective that fulfils their interests. Today, such processes are much more complex, but that does not mean they do not exist at all. In the end, they lead to *objectivization* and *externalization*; all the adopted institutions become somehow externally objective for us. If we do not adopt them into our lives we usually feel Hegel's sense of *alienation,*. Let's go back to the debate over the priest and imagine a rebelling actor in the medieval village; the result usually led to alienation and then exclusion from the society and exile or a death punishment. Who governs institutions made out of habits has power.

However, what kind of alienation can we feel in the environment of cyberspace, where most actors will never meet each other due to an enormous number of emerging (sub)cultures? We are usually alienated from a specific society, alienated from playing a specific *role*. Roles are important, as they are a certain actor's category of behaviour. By roles we fulfil others' expectations, our behaviour is predictable and by adopting it we feel less alienated, more socialized. However, we play many more roles today, in specific institutions but also in specific spaces of interaction – cyberspace. Sedimentation is a process of constant role-playing on specific layers – sediments – memory layers inter-subjectively internalized by, for example, language. During this process, institutions become more durable, as have languages for centuries. In that perspective, durability, constancy and stability are the core foundations of institutions of wider and less stable *social structures* (to be discussed later).

However, Bruno Latour made an important note here. He is convinced that all of the above described constructivist dynamics are not constant but fluid. His brilliant argument raises the question of how we can speak about a constant state of socially constructed society when construction is a process itself. Construction does not begin, does not end, it inflicts our lives as we have inflicted it. Then Latour adds technology as another actor into the process. In his meaning, technology development changes not only the technology itself, but also *the way we use it* (to be discussed thoroughly below). The constant flow of software updates with new features constantly changes the way we use it as well as new services, such as Google etc. The *way* consists of our habits and routines that change accordingly during the process of fluid change of social structures. Hence, it is not only ourselves who construct reality, but technology and its fluid continuous construction itself. A stable shape of social structures in time leads to trustworthy institutions, but cyberspace thanks to its fluid character does not easily provide us with such an advantage.

Cyberspace conceptualization would be approached as follows. Libicki's division of cyberspace into four layers provides a valuable perspective. There is no reason to fend all academic works dealing with problems that treat cyberspace as a mere network of computers or information systems. It is constituted of them on the first layer; they are operational on the second; containing the information on the third. The whole cyberspace conceptual framework discussed here is focused exactly and only to the fourth layer – the pragmatic or cognitive layer.[4]

Enhancing the Conceptual Framework With the Principle of Mutual Constitution

Drawing on the theory of social construction of reality introduced by Berger and Luckman in the 1960's, we assume that the cognitive layer does not or will not consist of one "global village" as proposed by Marshall McLuhan in 1990 (McLuhan 1990), but rather of much more decentralized social structures that have more or less influence on global society or globalization processes. There has been some criticism of the idea of a globalized interconnected world as being naïve, because this idea simply ignores global crises and catastrophes (Skidelsky 2012). The idea that connectivity directly implies a connected society is simply wrong. The opportunity to be connected follows a dynamic that is not new. Technology itself does not bring new principles, but new opportunities that are exploited the same way as before. Hence, developing and adopting habits and routines in cyberspace lead to an emergence of social structures and even more to the development of subcultures, but those do not need to be visible or available to join freely to the wide public; they are rather isolated and dedicated to selective people or groups – the principle of opportunity to be connected. Key knowledge or a selective interest is what

[4] The distinction between these two is unimportant as they are used interchangably in literature.

drives these communities and what empowers them. They may be cyberspace-only societies like guilds in MMORPG[5] or hacker groups breaking operating systems of world software leaders in hours after their release (Apple iOS would serve as an example), they may be societies consisting of hundreds of thousands of developers in open-source communities.

Each online community tends to develop its own norms and rules. Sometimes they are directly written as a condition to stay within the community; such rules usually serve to keep the community together, to avoid deviant behaviour. Hence, such expected habits are inscribed norms and thus constructs. Drawing on Giddens's theoretical framework of society's constitution of social structures referring to *"structural properties allowing the binding of time-space",* these properties are *"discernibly similar social practices"* that allow the social structures' *"existence across varying spans of time and space".* In that perspective, and according to Giddens, communities are less structures, but rather exhibit *social properties* in shape of *social practices* that in the end leads to *habits* and *routines*; the deepening process of practicing the social practices are *social principles* and long lasting structures practicing such social principles can be referred to as *institutions* (Giddens 1984, 17). Giddens proposes a very general theoretical perspective, which is greatly valuable while trying to understand the adoption of new practices that lead to encoded social principles in cyberspace. The continual existence of institutions is preserved by the adoption of habits and routines as a social principle referring to a particular social structure by actors and in the end by intended or unintended social control of such anticipated and expected behaviour. Cyberspace is fluid not merely due to a constant reconfiguration of its structure, but also due to a constant reconfiguration, and more precisely re-evaluation, of our habits. MySpace as a network centre would serve as an example – being sold for billions in the past, while having a minimum amount of users today due to users' preferences, habits and routines.

These social structures can be states as well as the above-mentioned cyberspace-only communities. In that framework, the *"deep structure of the state system exists only in virtue of certain rules and the performance of certain practices by states"* (Wendt 1987, 359); hence they are ontologically dependent upon their elements. States and systems are both construed and additionally they are each dependent upon one another; they cannot exist alone, it would lose sense. Anthony Giddens introduced this duality of structures to social theory by asserting that *"structural properties of social systems are both the medium and the outcome"* (Giddens 1979, 69) and additionally *"…of the practices they recursively organize"* (Giddens 1984, 25). However, Giddens's important contribution here is the conditionality that drives the inter-dependent ontological existence – the habits and routines (Giddens 1984, 19). Structure and practices are constructed mutually. The condition of mutual constitution links actors to structures constructed by actors into institutions, but according to Latour they would not last for a long time. It is a continuous fluid process of emergence and demise of structures made by actors, by technology and by both – *by the use of it*.

There is a social structure that would be identified as a nation situated on a particular territory and distinguished by language in cyberspace. However, those social structures dissolve or are becoming less significant due to raising trust in other social structures in cyberspace. The conventional division of rules, norms and habits along with national boundaries has been dissolved by the globalization process; it has not become a so-called Global Village, but rather a wide variety of alternative social structures that lie somewhere in-between the territory and thus an applicable law of a particular state in a virtual constructed world dissolves in seconds or years. Cyberspace constructs such social structures dependent on newly adopted routines, habits, rules etc. that, in the next step, challenges the world's normative regimes and thus contributes to the erosion of states, which may one day threaten world stability.

However, according to the Giddens's perspective of mutual construction of social structures, we can assume the lowering of the importance of daily routines and habits that have been intentionally or unintentionally developed within specific cultures. A society – a prime social structure – living on a particular territory, and thus, especially since 1648, within a particular state, leads to state erosion, if we accept the state as a constituted prime social structure. Social principles, such as the respect of territory of

[5] MMORPG (Massive Multiplayer Online Role-Player Games)(e.g. Salazar 2005)

others, are challenged if not physically then definitely on a cognitive layer. People have the right to free access to information; hence it is a norm that states cannot ban such a right – to censure. We found three important processes that can be studied within cyberspace-only social structures, that in the second step would significantly influence the debate over the normative regime in cyberspace between states: constitutive, influential and persuasive.

Three Processes Within Cyberspace Social Structures

Constitutive processes are deliberately oriented on the creation of principles that would last for a long period of time, are independent on the external world, or nowadays habits, and produce trust over its actors. The development of BitCoin (Nakamoto 2008) is exactly such a process. The existence of currency that is completely out of the control of any national bank, but people around the world trust it so much they have billions of dollars' worth of investments. Politicians and economists are very well aware of the risks such an emergence of digital currency brings to the stability of international exchange markets, and are trying their best to keep it under control, but with non-essential effects (Plassaras 2013). Constitutive processes have been seen in all ages and powerful people have had the tendency to put such processes under their control all the time. The emergence of cyberspace changes these centuries-lasting dynamics. Mark Zuckerberg changed the daily habits of communication of millions of people when he was 23; when he was 29 he influenced 1/5 of the world's population every day. If we go back just to the point of emergence of full-scale international business over the Internet, and especially using it as a method of payment, we might recognize a switch of where the taxes are collected. E.g. Apple bills us for buying applications for our iPhone in Luxemburg; hence, no taxes are paid in countries where the service is used. The application Uber providing taxi service all over the world is not only about taxi drivers, but it is also about the territory in which taxes are collected for services delivered elsewhere. We are witnessing an emergence of a whole social system where states are not playing their traditional role in both normative and economic dimensions.

Influential processes do their best to establish norms within traditional structures, such as states, according to new developments in cyberspace. Influential processes are those in which already well-adopted habits and respective actors understand routines and principles as norms and are convinced that the norm is already constituted enough that any challenging norm should be overthrown. For example, pirate political parties are convinced about the illegitimate accusation of people sharing data on the Internet. Pirates raise the argument of the human right to access information while ignoring the widely accepted norm of the right to ownership of intellectual property. Cyberspace-only societies and actors are adopting new habits that are thus adopted as a widely understandable norm. The national law of a particular state loses power over its territory; calling for obeying rules within cyberspace generated by a particular server is short-sighted. The possibility to move such servers to a territory that does not accept the norm of e.g. intellectual property is easy. The result is a habit of ignoring rules that were commonly accepted – intellectual property is one of the most crystal clear examples. We can find plenty of examples of how cyberspace social structures overgrow the normative framework of nation states simply by repeating a specific behaviour that led to the emergence of a norm and thus calling for a law update accordingly.

Persuasive processes can be understood as processes that deliberately try to persuade other social structures or their actors about their interpretations leading to trust them. They focus on the cognitive layer with manipulative information that does not need to be a lie, but favour the initial social structures. The difference from the influential processes is their tacit approach of influence. The target is usually not aware of the authentic reason of its existence. In another meaning, changing opinions, behaviour and decision-making of a particular social structure to favour the initial social structure can be referred to as an information operation.

Concluding Remarks

First, since the major social structures produce, and mutually depend on, our trust in the deployed political system, society has become more vulnerable in cases when those structures are significantly challenged. The stability of social structures is dependent on practicing our routines. The process of habitualization is challenged by cyber means and would lead to the dissolution of the traditional and law-embraced social system.

Second, when social structures are situated across borders, they are *cross territorial*, then states exercising their jurisdiction within their borders would not influence social structures that are past the border. Hence, norms accepted by people constructing such structures are becoming global. Technologies such as TOR or torrents based on the decentralization principle are important here, because they are a direct reaction to any rule-development efforts by authorities. Cyberspace as a fluid entity can immediately adapt to a newly established regime. Shutting down the data-sharing server megaupload.com in 2012 strongly increased the popularity of torrents that cannot be cut off.

Third, states are not the only entities to possess the honour of being rule-makers in cyberspace. There are emerging new entities that challenge the world normative regime. International law in the post-World War II state has represented bargains between states seeking world stability and as such has represented part of an accepted social structure of states – a normative regime. The indistinct use of force in cyberspace (Ziolkowski 2012) possesses a serious threat of such regime development in cyberspace. Nevertheless, due to the fact that there are more agents than states that may significantly influence the normative development in cyberspace we have to take into consideration other agents as well. The current debate of norms in cyberspace is strictly focused on the mutual behaviour of states, especially on the use of force and other aspects of humanitarian law. However, regulation of states' behaviour does not affect non-state actors. The cases of whistle-blowers would serve as an example as they are capable to significantly influence our perception of an appropriate and thus normatively accepted behaviour.

Fourth, we may observe a so-called dual-interest of states when they exploit attribution of a problem to cover their activities. On one hand the current situation drives states to develop a regime that would shape cyberspace into a secure environment to secure e.g. critical infrastructure and to keep all components of modern society together, and on the other hand, it drives states to maintain a status quo because it provides an unprecedented tool for intelligence-gathering, propaganda, precise sabotage attacks and thus an opportunity to gain a strategic advantage. States thus play the role of non-state actors.

Conclusion

This article used a classical sociological constructivist perspective to conceptualize the cognitive layer of cyberspace. It focused rather on the dynamics of actors in cyberspace as social structures and analysed consequent outcomes than on commonly discussed cyberspace security topics. However, such an approach seems to be valuable when evaluating the emerging power of non-state actors as new alternative social structures based on our habits and routines as well as preferences that lead our decisions during the use of ICT. We found several processes that constitute (digital currencies) those structures; influence the other structures by pushing new appropriate behaviour in cyberspace (intellectual property), and persuade other actors through precise information manipulation. The significance of structures lies in their level of institutionalization by a system of rules or tools (constitutive process) and the actors' trust. The final conclusion of the article points to a possible process of the erosion of the state fuelled by prevailing constitutive processes of alternative social structures in which actors trust. In that perspective, society is much more fluid as our cognitive reflection is fluid as well, because the whole cognitive layer is fluid. This moment, however, may be just a switch into a more stable society. The article, though, tried to argue that the opposite is more plausible, because the strength of institutions depends on our trust into the constitutive social structures that are much more fluid in cyberspace than ever before.

Jakub Drmola

Introduction

Probably everyone has encountered some form of anti-piracy campaign or advertisement. They are as prevalent as piracy itself - there are stickers, logos on boxes, short advertising spots before films start in the cinema, warnings on DVDs, online banners, and many other forms. For many years now, copyright holders and content creators have been struggling to convince both the public and governments that piracy is harmful and that it is worth fighting against.

The technological progress, however, has not been on their side. Rapid proliferation of devices capable of processing digital data coupled with the ever faster and ever more ubiquitous Internet connection is making piracy easier and more appealing year by year. It seems like only yesterday when friends would borrow their worn-out magnetic cassette tapes from each other to copy songs. Nowadays, even DVDs are quickly becoming obsolete, despite being unimaginably faster, of higher capacity, more reliable, and cheaper. It is simply too slow and cumbersome to physically move them when you can just transmit the data down the wire or through the air. Large amounts of data, exceeding what used to be an entire computer storage capacity twenty years ago, are transferred as part of regular background updates within minutes today. It is no wonder that these incredible capabilities are being used to disseminate and distribute all kinds of digital content, including the one that infringes on someone's copyright (Tassi 2012).

To counter these unfavorable developments, companies being negatively impacted by piracy had to evolve and improve their anti-piracy efforts to make them more effective, compelling, and persuasive. The securitization of piracy has been, in some sense, the highest and most escalated form of this process. It was of course never openly named as such, but there has been a noticeable shift (or rather parallel expansion) towards a more serious and security-related discourse surrounding piracy. How and why that happened is what this text seeks to elucidate. But first it is necessary to delve into what piracy even is and why it matters.

What is Piracy and What Does It Do?

Piracy in the non-maritime sense is often defined as "unauthorized use or reproduction of another's work".[1] It can also be seen equated to terms as varied as the legalese *copyright infringement*, *intellectual property theft* one the hand, and *intellectual property sharing* on the other. It is considered to be a serious crime by some and a benign necessity of modern life by others. Sometimes, the content is offered for profit, sometimes just for bragging rights. Some authors include industrial espionage and counterfeiting of goods into piracy, while many do not. This article focuses on the so-called *online piracy*, which is when unlicensed and unauthorized copies of digital media are created and transferred over interconnected networks.[2] That means it excludes both counterfeiting and physical copying, but that does not make it any less complex.

The lack of a clear consensus on what exactly piracy is, is not the only problem. There are major disagreements regarding its causes, its effects, and even whether it is a generally good or bad thing. And there is, of course, even less agreement on what to do about it and what its future will or ought to look like.

[1] See: http://www.oxforddictionaries.com/definition/english/piracy.

[2] As noted in the introduction, piracy has existed in different forms since even before the internet proliferated. The history of media piracy is far more ancient than just the copying of magnetic tape cassettes (VHS or MC/CC) at home. It can actually be traced back to seventeenth century book printing (see Balazs 2011, Johns 2013).

Consider the case of HBO's Game of Thrones, which is the world's most pirated TV show of all time. Some of its episodes recorded up to one million downloads within their first day of being available on the BitTorrent network with almost 200 thousand users sharing it (i.e. offering it for free to anyone) simultaneously. The season four finale broke all previous records with 1.5 million downloads within 12 hours and 250 thousand people sharing the file (Ernesto 2014). Conventional wisdom would dictate that this is terrible news for the producers of the show because they are losing their money when people all over the world watch their product without paying for it. Yet HBO executives are apparently not overly perturbed by this. Some of them even go as far as to praise the piracy and claim it is good for their show as it provides free publicity which allegedly does not hurt their DVD sales (Hibberd 2013, Ross 2014).

But these statements were, quite understandably, contentious and criticized. Other authors and executives see things differently and do not consider piracy to be "benign" or a "symptom of success". Gale Anne Hurd, producer of another highly successful TV show The Walking Dead, worries about the long-term sustainability of the creative process amidst high piracy rates - these shows are not cheap and someone has to pay for them in order for them to be made (Sweney 2014), and she is by far notalone with this opinion. There are voices of disagreement even within the Game of Thrones franchise. The show runner, David Benioff, mused (Isidore 2013) that if all those people who download it online paid instead, he could afford better visual effects and more scenes with dragons.

This very brief introduction illustrates how complicated the issue of piracy is even within the industry itself. And this example covers only a very tiny subset of the whole. Films are pirated too, of course. The music industry is another huge domain which also needs to cope with piracy but which runs on an entirely different business model. Finally, there is software piracy which covers everything from operating systems and productivity suites to video games. And according to The Software Alliance study (BSA 2014), nearly half of all software installed on computers worldwide is "not properly licensed".

Another layer of complexity is added when it comes to the actual act of copying and transmitting (i.e. downloading) the data. But even when technicalities are disregarded, the effect piracy has on individual industries is not clear-cut and remains highly contentious (Danaher and Waldfogel 2012, Poort and Leenheer 2012, Ross 2011, TERA 2010, Oberholzer-Gee and Strumpf 2010).

The Role of Piracy

Piracy has become an important aspect of current cyber culture. Probably the most pertinent symbol of this is The Pirate Bay - a website which hosts a large and searchable BitTorrent directory. It does not host the content directly, but it provides means for users from all over the world to download various files from one another other, which forms the basis of the decentralized peer-to-peer data transfer.

What makes The Pirate Bay, founded in 2003, special and significant is not its content or its size but that it has been at the center of both legal and cultural struggle over online piracy. Over the last ten years it went through a lengthy trial, a police raid, numerous DDoS attacks on its servers, access to it has become blocked in several countries[3], and it has generally been the primary target of anti-piracy campaigns and at the forefront of the raging debate.

During the same time period, it grew to become a cultural focal point and a potent symbol for not only piracy specifically but also for the more ephemeral "fight for the freedom of the Internet" in general. This was most visibly manifested in hacktivist campaigns when the Anonymous movement launched DDoS attacks against notable anti-piracy organizations and performed defacements of their websites. The biggest of these "anti-anti-piracy" campaigns on behalf of The Pirate Bay was the so-called "Operation Payback (is a Bitch)", which started in September 2010 (Ernesto 2010) and continued until December,

[3] This blocking of The Pirate Bay and other piracy-facilitating websites is most often done by the local Internet Service Providers after being compelled by a court order. However, efficacy of this blocking is often questioned as it can be quite easily circumvented and the publicity this provides can even lead to an increase in the number of visitors to the site (Enigmax 2012, Clark 2012, Poort et al. 2013). In some countries, this lack of clear results has led to the blocks being repealed (BBC 2014c, Essers 2014).

when it eventually morphed into and was overshadowed by "Operation Avenge Assange" in support of the WikiLeaks whistleblower.

The second largest hacktivist campaign supporting online piracy as a form of Internet freedom had a rather unimaginative name, "Operation Megaupload." This took place in January 2012 and was a reaction to the shutting down of the popular Megaupload file hosting service and impounding of their servers (which held all the users' data). As before, mostly copyright advocacy organizations and various government institutions were targeted and disrupted during the protest. This campaign then gradually segued into the global anti-ACTA and anti-SOPA protests. These protests shared the "freedom of the Internet" skein but they were not about piracy specifically. Even aside from these major protest events, piracy remains a key issue and one of the most frequent causes for disruptive political cyber attacks all over the world. These can be often observed during and after piracy-related court cases or legislative proceedings (for example Andy 2014).

The prominent position of The Pirate Bay was even leveraged by the Swedish Lund University (de Kaminski 2013) to facilitate its research on "cybernorms" and demography of online pirates[4] and the website itself frequently supports and promotes causes of a political nature (such as ongoing protests, elections, trials and others). The other consequence of The Pirate Bay's central position and the ongoing struggle to keep it up and running is its remarkable resilience. It has been growing more and more decentralized over the years, switching domains and national jurisdictions regularly, bypassing blocks and looking for ways to minimize both its physical and legal footprint. These measures include moving all of its content to cloud services to prevent further police raids (Kerr 2012) and also shifting away from hosting .torrent link files in favour of using the so-called "Magnet links" instead (Meyer 2012).

The continuing pressure from anti-piracy organizations and state institutions has in effect turned The Pirate Bay into a major cultural and political symbol of "Internet freedom", thus entirely eclipsing its original position and impact on cyberspace security. It attracts extra publicity, more visitors, and makes its supporters much more numerous and willing to fight to keep it online purely because of its emblematic value. This, combined with The Pirate Bay's forced evolution towards an ever-greater technical resilience, means that it is now much more difficult to get rid of than when it was "just another piracy website."

Another notable manifestation of Internet piracy as a cultural and political phenomenon is the recent emergence of various Pirate Parties. Started in Sweden in 2006 as a direct reaction to The Pirate Bay's ongoing legal woes it soon inspired namesakes to crop up in many other countries. But despite some initial success, Pirate Parties remain a minor political force and currently do not possess practical influence over national policies or security issues.

The Second Enclosure Movement

While the ordinary and everyday continuance of piracy and the campaigns against it might seem rather mundane and mostly driven by definite interests and grievances of particular actors, there is also a high-level and abstract overarching idea complementary (some might say antagonistic) to the aforementioned fight for the "freedom of information." Called the Second Enclosure Movement, it uses a reference back to the original "first" Enclosure Movement of 18th and 19th century England and Wales, when previously common pastures[5] were "enclosed" and turned into a privately owned land in order to increase productivity and prevent overgrazing (Kain, Chapman and Oliver 2004). Economic and food security were one of the main arguments in favour of enclosing the commons.

Whereas the original Enclosure Movement concerned fields and pastures, the Second Enclosure Movement is a name given to the ongoing effort to "enclose intellectual commons," predominantly by the critics of this process. One of the most notable scholars pursuing this idea is James Boyle (Boyle 2003).

[4] Searchable results are available on: http://www.thesurveybay.com/index.php.

[5] This concept was used in the economic theory by Garret Hardin called Tragedy of the Commons much later (see Fairlie 2009). It posits that the rational self-interest of individual actors leads to the squandering and depletion of common resources and expands this general "rule" from pastures to many other areas.

The main line of criticism is targeted against the eroding of limits on intellectual property rights and expanding the spectrum of knowledge which can be thus protected and removed from the public domain.[6]

Supporters of this movement argue that this expansion is necessary in order to stem the tide of piracy and copyright infringement, to promote innovation, and to safeguard economic growth in knowledge intensive industries. In light of this conceptual approach, it is possible to see Internet piracy as a major battleground between proponents and opponents of the second enclosure in one particular sector. The securitization of piracy serves to advance and promote the cause of enclosure as something essential and beneficial to the society at large (Ertuna 2009).

What is Securitization

Unlike piracy and the campaigns surrounding it, securitization is a well-established concept within the domain of international relations and security studies. It is therefore easier to make use of what has already been written on it. Securitization is simply an act of labelling something as a security issue (Taureck 2006). Among other things, this implies that it is (inter)subjective and socially constructed. In other words, what is considered to be a security threat largely depends on the actions and perceptions of people, not on some material and objective indicators of insecurity (Sulovic 2010).

The process elevates (or attempts to, at least) the issue above the normal political discourse. Once something is successfully securitized it is perceived to present an existential threat to whatever value needs to be protected. Such a threat also requires accelerated and resolute measures to deal with, together with additional resources. There are many examples of this process. Sometimes it happens almost instantly and the threat seems obvious, which is usually the case of wars, terrorism, or economic depression for example. In other cases, the process can be significantly slower, disputed, or even not entirely successful, such as with global climate change, migration, certain drugs or weapons (Maltman 2013).

This concept consists of three distinct components. The "referent object" is what is being threatened and what needs to be secured. The "securitizing actor" is the actor instigating and supporting the process. And finally, there is the audience which may or may not be convinced by it. To put it very crudely, the securitizing actor basically tries to convince the audience that the referent object ought to be protected and that additional measures are required to do so.

This framework can be quite straightforwardly applied to piracy. Securitizing actors are mostly the companies whose content is being reproduced without proper authorization and various organizations (national or international) who represent them. The audience is either the public, which chooses whether or not to participate in piracy, and, more importantly, governments and institutions. Because it is them who create and enforce rules and laws and thus shape the environment within which piracy occurs and, supposedly, also have the most power to curtail it. Interestingly, while piracy as a source of threat remains constant, the choice of the referent objects (i.e. what is being threatened) varies. It ranges from the value of art itself, to economic security (mostly through loss of jobs and disincentivization of innovation), to internal order and public security.

The Fight Against Piracy

Before exploring highly securitized debates surrounding piracy and the struggle against it, it is necessary to take at least a succinct look at the "normal", or the non-securitized, arguments. This paves way for possible comparisons and also makes sense from the chronological point of view, as securitization followed after the relative lack of success of earlier efforts. These non-securitized arguments or campaigns are targeted predominantly at end users. End users can be either paying customers who are being targeted in order to prevent them from turning to piracy, or active pirates which

[6] The main argument generally is that, unlike pastures, data and knowledge are intangible and therefore cannot be depleted by their common use.

ought to be dissuaded from their activities and turned into paying customers. In reality, of course, it is a mix of the two.

One of the most common arguments is that the act of piracy, i.e. not paying, is destroying the artist's ability to make a living, thus "killing" the art itself.[7] If this were to be allowed to continue unchecked, the argument goes, there would be nothing much left to either see, buy, or download, as most of the artists, designers, and software programmers would have to move on towards other careers. Instead, they deserve to be supported and rewarded for work they do and the value they provide. The bottom line is, that by participating on piracy one might be financially hurting the authors of the content he or she likes and enjoys and thus preventing more of it from being produced.

Very closely related is the argument about ethics and morality. In some cases, piracy is being equated with theft of physical property - an act considered immoral by most. It is basically an appeal to personal or group ethics saying that if one considers physical stealing to be wrong then one should treat piracy the same and refrain from doing also.

On a more practical level, this directly ties into the legality of piracy (or rather the lack thereof) and deterrence by punishment. Piracy is often illegal and occasionally can result in fairly high fines or even imprisonment (depending on the specific country). The detractors of piracy argue that access to free content is not worth the risk of prosecution.

In practice, however, the impact of these arguments and campaigns is quite limited. First of all, the ability and will to enforce laws against piracy is generally quite low. Given the very low chance of any given pirate being prosecuted (especially if some anonymizing protective measures are adopted, such as VPNs or blacklisting), the deterrent effect is not particularly strong. Additionally, pirates maintain that piracy should not be considered a theft, because the original "item" is not being removed or destroyed due to its digital nature. They prefer terms such as copying or even sharing.[8]

Piracy advocates also point to the long history of piracy and the apparent lack of any sign of it having devastating effect on creative industries claiming that they are continuing to flourish instead (Cammaerts, Mansell and Meng 2013, Enigmax and Ernesto 2011). To make matters even worse for anti-piracy campaigners, a subset of artists themselves speak up against the current copyright system and consider piracy to be a relatively benign phenomenon (as was noted earlier), which further undermines the argument about piracy killing art. It also allows pirates to see the unpopular multinational corporations as the ones suffering the losses instead of the artists. In the end, pirates generally do not consider themselves to be criminals, do not fear prosecution, and are not too worried about killing anything.[9]

The other common arguments against piracy focus on the content itself. Due to the unofficial, often illegal and even disreputable means of obtaining it (i.e. downloading it from untrustworthy websites or directly from other people), it can contain malware which then infects the pirate's computer and causes them further loss, financial or otherwise (Gantz et al. 2014). Another common criticism, almost exclusive to the piracy of films and TV shows, is that the content thus obtained can be, and often is, of inferior quality. In more extreme cases it might be some other video entirely, instead of what it purports to be.

The opposition maintains that these claims are being overstated (Hawes 2014), but getting any real measurement on how dangerous malware embedded in pirated software is or how likely one is to get infected by it is exceedingly difficult. A more common problem is that the pirated software often lacks regular patches and security updates released for properly licensed versions, which makes it more vulnerable to malware and other kinds of attacks. It is similarly difficult to deal with the issue of quality, since it is being offered for free, and the end user himself has the ability to pick and choose what he deems worth downloading or not. The ever-increasing transmission speeds are also gradually changing the situation as more high-quality videos are becoming widely available.

---

[7] A very creative example of this sort of campaign can be seen at: https://torrentfreak.com/piracy-virus-kills-elvis-hendrix-marley-mercury-morrison-110425/.

[8] See: http://www.vincentchow.net/wp-content/uploads/2008/09/piracy.png.

[9] Examples of this kind of anti-piracy posters and logos available at: http://www.digital-digest.com/news-63369-Pictures-of-the-Week---A-Look-Back-At-Anti-Piracy-Ads.html.

In the end, it is quite possible that all of these arguments against piracy were doomed to fail from the very start simply because they were targeting the same demographic which stands to benefit from piracy the most.

Piracy as a Security Threat

The following two approaches to treating piracy as a security threat have not displaced the original and more common lines of reasoning described in the previous chapter. They have become more or less complementary. The securitization of piracy plays essentially two roles. Primarily, it shifted the focus away from personal ethics and negative consequences towards impacting the entire society or nation. It argues that piracy poses a threat not just to a pirate's individual conscience, finances and his computer, but that it also severely threatens everyone else in the country. Therefore, pirates and the copyright owners cease to be the sole parties of this struggle.

Secondly, it suggests that the negative consequences of piracy are much graver. While the dangers mentioned in the previous chapter can be hardly considered security threats in the true sense of the word, securitization suggests that piracy can pose a real risk to people's lives and livelihoods. A combination of these two ideas pull national governments into the argument.

Hard Security

The first, and probably the most disturbing and controversial, attempt to securitize piracy took place on the backdrop of increased international interest in terrorism, during the so-called "Global War on Terror". News reports, articles and studies (Seenan 2004, Lettice 2004, McCullagh 2005) were suggesting a link between piracy and terrorism, and claiming that terrorists use piracy to fund their violent activities. This implied that users partaking in piracy are in effect assisting terrorists - an idea gladly adopted by some anti-piracy campaigns.[10]

This was gradually expanded to include trafficking (of both goods and people) and organized crime in general (IFPI 2004). A notable study was released by RAND (Treverton et al. 2009), supporting these claims and citing several case studies of counterfeiting being used to fund organized crime. Further, similar studies followed by various other organizations (such as Smith et al. 2011). It is hard to imagine a claim more serious than a direct link to terrorism. Therefore, if accepted, this link would be a very strong argument for a resolute action against piracy.

However, all of the aforementioned studies and reports were strongly criticized and their methodology was found wanting. Most commonly alleged issues were mixing piracy together with counterfeiting of physical goods (such as clothes or medical drugs), inflating numbers, providing very tenuous causal links and being funded by anti-piracy organizations (Jones 2009). The most comprehensive "counter-study" was produced by Social Science Research Council (Karaganis et al. 2011), tracing the evolution of these reports and directly attacking their claims about profitability. According to SSRC, sales of pirated CDs and DVDs are suffering from falling margins for the same reason as the legitimate industries - proliferation of the Internet and the ability to download their content directly.

Overall, the idea of piracy as a security threat, due to it being used to fund terrorism and violent crime, did not get too much traction, mostly due to sparse and ambigous evidence. Also the fact that it was targeted at audiences in modern and developed countries, where the sale of pirated optical discs is mostly a thing of the past, due to the proliferation of high-speed Internet, did not help the case. Nevertheless, the proposed link to organized crime still resurfaces every now and then and remains embedded in the ongoing debate (Anderson 2011a).

[10] See: http://www.digital-digest.com/images/newsimages_ftp/terrorist_dvd_piracy.gif.

Economic Security

The second wave of piracy securitization came about during the global financial crisis, starting in 2007. Capitalizing on the ongoing economic downturn, it focused on the broad and far-reaching negative effects of piracy on national budgets and employment. This was a notable shift from the original claims of piracy damaging music or film industries specifically, towards piracy threatening the entire economy in general. It was, yet again, supported by a number of studies, the majority of which claimed at least tens of billions of dollars of losses for national economies and hundreds of thousands of lost jobs. The most prominent and widely cited of these studies focused on US economy (Siwek 2007), others on the EU (TERA 2010) and several treated the issue on a more global level (OECD 2008, BSA 2012). The prospect of digital piracy causing people to lose their jobs at a time of economic recession was especially significant. This has moved the entire debate towards economic security and stronger involvement of governments.

Predictably, these studies and reports became highly criticized, largely for the same reasons as the ones suggesting a link between piracy and organized crime. The methodology of calculating losses has been especially contentious leading to widely varying estimates. Allegations of repeated counting, inflation of numbers, and unfounded estimates were rife. Apart from SSRC (Karaganis 2010) and journals (Sanchez 2008, Bialik 2013, Masnick 2013), even the United States Government Accountability Office voiced its scepticism regarding these figures (GAO 2010).

The basic idea of piracy harming the economy still remains in the discourse, more so than the notion of terrorism being financed by piracy (Anderson 2011b). In this sense, economic securitization of piracy can be considered to be a more successful case than the previous one, perhaps due to ongoing economic woes being closer and more "real" to the audience than terrorism. Some of the same arguments were also echoed during the debate surrounding SOPA, PIPA and ACTA.

Conclusion

From timing alone it is apparent how the securitization process can be contingent upon seemingly unrelated political events. Both attempts to securitize piracy tried to make use of major security concerns of the day (terrorism in one case, financial crisis in the other) in order to make the anti-piracy arguments more compelling, which was sorely needed since the regular appeals to ethics and love for art failed to reverse the trend. They achieved mixed success nevertheless.

It would also seem that any effort to link piracy to some already recognized and acknowledged security threat was undertaken simply to convince an audience (public or governments) that additional measures are warranted to fight piracy, not in attempt to curb terrorism or restore financial markets. This is supported by the fact that all the studies and reports contributing to this debate (arguing for either side) were of media, copyright, or digital culture provenience. A paper authored by an established terrorism researcher claiming that the fight against terrorism requires stricter copyright laws is yet to be seen.

While some claims about the threat that piracy poses to nations and society might seem questionable, other threats remain overlooked. Curiously enough, these neglected threats might even be more palpable and suitable for securitization for their own sake than the two elucidated above. The political and cultural role of piracy has already been explored in one of the initial chapters of this article. Its potential as a mobilizing agent for hacktivism should not be overlooked, yet it is usually ignored when it comes to debates about copyright and impacts of piracy on society. The danger of underestimating this side of piracy has already been demonstrated on several occasions, and while the impacts have not been too severe, the cost of repeating this mistake will only grow with time as the society becomes ever more dependent on information and communication technologies.

The second, and arguably more practical, security threat stemming from piracy has been mentioned here only very briefly, because it is only rarely invoked during anti-piracy campaigns. It is the case of computers being vulnerable to malware or hacking because of the lack of patches, security

updates and timely support. In the current highly dynamic environment of perpetual cyber attacks against virtually all kinds of targets, it is absolutely crucial to maintain systems updated and protected. Since pirated software often lacks these regular updates (not always though), it presents an easy target and point of entry into sensitive networks, especially on the corporate and institutional levels. Moreover, a significant proportion of botnets is created through the use of malware embedded directly into pirated operating systems downloaded over the Internet or even pre-installed on PCs sold in fraudulent shops (mostly in developing countries). Botnets are then used for DDoS, phishing or brute-force attacks, thus having a substantial negative impact on global cyber security (Finkle 2013, Greene 2012). In light of these threats, the ongoing piracy securitization efforts seem rather misplaced.

Closing remarks

The breadth and scope themselves clearly demonstrate how omnipresent and ubiqitous cybersecurity has become. Barely any facet of our existence has been left untouched by it. From commerce and entertainment, to espionage and terrorism, cyberspace has become interwoven with the fabric of human society as much as printed text.

It is also quite telling, that we seem to be repeatedly struggling with the same issues over and over again. While the context may have changed together with the year shown on our calendars, we are still wrestling with exactly the same problems we have been during the Cold War or even the first half of the 20th century. One might argue that even the ancient Greeks were debating the same questions and fighting over the same values as we are now.

We remain wholly uncertain how to balance free speech, democracy, security, economic prosperity, social justice and national sovereignity against each other. It is quite possible, indeed probable, that no permanent or perfect balance can be found at all. No matter how hard we might try and how close we might come, there will always be some new source of disruption, some new technology, that will upset the balance once again, shattering our presumptions and exposing our hubris. Right now, this role is filled by the Internet and the digital revolution. And we are not sure what lies over the horizon.

But this must not discourage us from trying to understand it better. We are learning more with every passing year. We are gradually coming to grips with our current social reality. We are slowly discovering the most adverse imbalances. We are trying to figure out better solutions to our enduring difficulties. We will not get it perfect, surely. But we can make it gradually better. Or, at the very least, we ought to be able to prevent our circumstances from getting worse.

On top of elucidating their particular areas of interest, diverse chapters found in this book show that the way forward leads through a multidisciplinary research. Just as cyberspace does not touch just one area of our lives, there is no single scientific discipline or method that can answer all the questions we have about it. We must bring together political science, law, psychology, economics as well as mathematics and technical disciplines to ensure extensive crosspolination of ideas which will hopefully lead us towards better understanding of the impact that the emergence of cyberspace has had (and will have) on our society and culture. Approaches presented in this book will hopefully act as an instructive illustration of the diversity of this field to future scholars, who might find some inspiration in the issues and cases covered here.

This is neither the first, nor the last step in the right direction, but one of many important steps nonetheless. More books need to follow, more research needs to be done. Furthermore, cybersecurity needs to become a public issue and a common interest of all.

Lucie Budírská

Lucie is a Ph.D. student of International Relations at Masaryk University in Brno. She is interested in connections and links between international relations and cyberspace. In 2012 she spent one semester at Missouri State University in Washington, D. C. where she attended the course "Cyberspace and American Power" led by Prof. Eric Sterner.

Jakub Drmola

Jakub is an internal Ph.D. candidate for the Security and Strategic Studies section at the Department of Political Science at Masaryk University in Brno. His main research interests are actors and threats of cybersecurity, asymmetric conflicts, impact of modern technology on security, and application of system dynamics to these issues.

Jakub Harašta

Jakub is an Assistant Lecturer at the Institute of Law and Technology, Faculty of Law, Masaryk University and a Visiting Research Fellow at Minerva Center for the Rule of Law under Extreme Condition at the Faculty of Law, University of Haifa. His research focuses mainly on legal framework for cyber security of critical infrastructure and legal issues of penetration testing and electronic evidence. Jakub obtained his Master degree in law (Mgr.) in 2013 and his Doctor of law degree (JUDr.) in 2015. He currently pursues his Ph.D. in Information and Communication Technology Law.

Lea Hricikova

Lea became interested in cyber security as a student of the LLM Law and Politics of International Security at the Vrije Universiteit Amsterdam (from which she graduated in July 2013), since the topic exposes both political and legal issues. During her internship at the Institute of Defence and Security Studies in Bratislava she wrote a policy study on the initiatives of the Slovak MoD in cyber security (in the Slovak language). Later she submitted a paper on the legal challenges attached to the surveillance and monitoring technology for internal circulation as a volunteer external researcher for the European Centre for Information Policy and Security and represented the Centre at the Computer Defence and Network Security conference in London (January 27-30). She has previously been a student of BA (Hons) War and Security Studies at the University of Hull.

Alena Leciánová

Alena Leciánová studies Security and Strategic Studies (MA) at the Faculty of Social Studies of Masaryk University in Brno. In her studies, she focuses on the field of advanced technologies, especially on information and communication technologies and their implications for protecting or threatening not only nation-state security.

Tomáš Maďar

Tomáš is a student of Security and Strategic Studies at the Faculty of Social Sciences of Masaryk University in Brno, Czech Republic. He focuses on theoretical cyber security, organized crime, and geopolitics.

Miroslava Pavlíková

Miroslava is a graduate student of Security and Strategic Studies at Masaryk University. She is interested in cyber security, terrorism, extremism and security issues of the Euro-Atlantic region and Russia.

Nikola Schmidt

Born 1982 in Prague. Previously director and co-founder of a software development company also operating in the field of IT security. Currently a PhD candidate at the Department of International Relations, Institute of Political Studies, Faculty of Social Sciences, Charles University. His research interests are focused on perspectives of cyberspace regime development. He graduated from the Metropolitan University in the program of International Relations and European Studies. He specializes in critical analysis of cyber space, cyber security and cyber war. His other interests concern the field of space security and intelligence. From the broad perspective, he focuses on international security and the role of new technologies in its dynamics. His research is focused on cyber space, cyber war and space conceptualization. He is currently working on supported research concerning the application of classical theoretical approaches of strategic deterrence to asymmetrical threats of cyber space.

Petr Suchý

Head of the Department of International Relations and European Studies, Faculty of Social Studies, Masaryk University, Brno, Czech Republic. He mostly focuses on the American Security and Foreign Policy, Cold War strategy, Reagan administration, nuclear weapons and disarmament.

Roman Šulc

Roman graduated from Security and Strategic Studies at Masaryk University, Brno. He focuses on cyber security/emerging risks from technologies and new religious movements.

References

AfricaItNews. 2013. “ZTE and Huawei Accused of Spying: A Threat to Africa?“ AfricaItNews, May 27. http://en.afriqueitnews.com/2013/05/27/zte-and-huawei-accused-of-spying-a-threat-to-africa/

Aggarwal, V., K. and M. G. Koo. 2008. “Asia’s New Institutional Architecture: Evolving Structures for Managing Trade, Financial, and Security Relations.” Springer (2008):31. http://link.springer.com/chapter/10.1007%2F978-3-540-72389-9_1?LI=true

Agora. 2012. “Niesvoboda interneta.” http://www.eliberator.ru/files/АГОРА.%20 Несвобода%20Интернета%202012.pdf

Ahrens, Nathaniel. 2013. "China’s competitiveness Myth, reality and lessons for the United states and Japan, Case study: Huawei." Washington: Center for strategic and international studies. http://csis.org/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

Albert, Jacob. 2012. “Trusting Huawei.“ The American interest, February 27. http://www.the-american-interest.com/articles/2012/10/31/trusting-huawei/.

Albright, David, Brannan, Paul, and Christina Walrond. 2010. “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Alder, John 2007. In: Thiel, Marcus. 2009. "The Militant democracy principle in Modern Democracies." Farnham: Ashgate.

Alvesson, M, and K. Sköldberg. 2009. "Reflexive Methodology: New Vistas for Qualitative Research." SAGE Publications.

Amnesty International. 2013a. “Russia amnesty law no substitute effective justice system.” https://www.amnesty.org/en/articles/news/2013/12/russia-amnesty-law-no-substitute-effective-justice-system/

Amnesty International. 2013b. “Russian constitution 20 years continuing erosion rights and freedoms.” http://www.amnesty.org/en/news/russian-constitution-20- years-continuing-erosion-rights-and-freedoms-2013-12-12

Anderson, Nate. 2011a. “Major report debunks alleged link between piracy and terrorism.” Ars Technica, March 16. http://arstechnica.com/tech-policy/2011/03/even-commercial-pirates-now-have-to-compete-with-free/

Anderson, Nate. 2011b. “White House-backed antipiracy video is Reefer Madness for the digital age.” Ars Technica, November 30. http://arstechnica.com/tech-policy/2011/11/white-house-backed-antipiracy-video-is-reefer-madness-for-the-digital-age/

Andress, Jason. 2011. “Advanced Persistent Threat: Attacker Sophistication Continues to Grow?“ ISSA Journal. Vol. 9, no. 6: 18 – 24. http://polyhack.com/wp-content/uploads/2012/04/Andress-Advanced-Persistent-Threat1.pdf

Andy. 2014. “Hackers Turn Music Industry Site Into The Pirate Bay.” TorrentFreak, July 1. http://torrentfreak.com/hackers-turn-music-industry-site-into-the-pirate-bay-140701/

APEC TEL. 2010. “APEC TEL Strategic Action Plan: 2010-2015.”Adopted on the 8th Ministerial Meeting on telecommunications and Information, 2010. http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2010_tel/ActionPlan.aspx

Arimatsu, Louise. 2012. “A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations.” In The 4th International Conference on Cyber Conflict, Czosseck, C., Ottis, R, Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications. http://www.ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf

Arquilla, John, and David Ronfeldt. 1993. “Cyberwar is coming!” Comparative Strategy, Vol. 12, No. 2 (Spring 1993), RAND reprint: 23–60. Online: http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

ASEAN Secretariat. 2013. “ASEAN’s Cooperation on Cybersecurity and Against Cybercrime.” Presented at the Octopus Conference, Strassbourg, France, December 4, 2013. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/ASEAN's_Cooperation_on_Cybercrime_and_Cybersecurity.pdf

Asia-Pacific Economic Cooperation. 2013. “Key APEC Documents 2013.” Singapore: Secretariat.

Aslan, Adil, Celik, Eyyup, and Murat Dogrul. 2011. “Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.” In International Conference on Cyber Conflict, Czosseck, C., Tuygu, E. and Wingfield, T. (eds.). Tallinn: NATO CCD COE Publications. http://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf

BAE Systems. 2014. “Snake Campaign & Cyber Espionage Toolkit.” http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper_v7.pdf

Balazs, Bodo. 2011. “Coda: A Short History of Book Piracy.” Social Science Research Council, June 2011. http://piracy.americanassembly.org/wp-content/uploads/2011/06/MPEE-PDF-Coda-Books.pdf

Balík, Stanislav. 2007. “Totalitní a autoritativní režimy.” In: Demokracie. Teorie, modely, osobnost, podmínky, nepřátelé a perspektivy demokracie. Eds. Hloušek, Vít and Kopeček, Lubomír. Brno: Mezinárodní politologický ústav Masarykovy university.

Ball, Desmond. 2011. “China’s Cyber Warfare Capabilities.” In: Security Challenges, vol. 7, No. 2, 81-103. http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.

Barbash, Fred, and Ellen Nakashima. 2014. “Chinese hackers may have breached the federal government’s personnel office, U.S. officials say.” The Washington Post. July 10. http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/

Barboza, David. 2011. “Motorola Solutions and Huawei Settle Claims Over Intellectual Property.“ The New York Times, April 13. http://www.nytimes.com/2011/04/14/technology/14huawei.html?_r=0.

Barabási, A. L. 2002. "Linked: The New Science of Networks." Perseus Pub.

BBC. 2011. “Russia´s President Medvedev Denounces cyber-attack.” http://www.bbc.co.uk/news/world-europe-13011540

BBC. 2014a. “Russia enacts draconian law for bloggers and online media.” http://www.bbc.com/news/technology-28583669

BBC. 2014b. “Driverless cars could change everything.” http://www.bbc.com/news/blogs-echochambers-28376929.

BBC. 2014c. “Spain lifts blocks on file-sharing websites”. BBC News - Technology, July 18. http://www.bbc.com/news/technology-28367990

Beaumont, Peter, and Nick Hopkins. 2012. “US was ‘key player in cyber-attacks on Iran’s nuclear programme’.” The Guardian. June 1. http://www.theguardian.com/world/2012/jun/01/obama-sped-up-cyberattack-iran?newsfeed=true

Bejtlich, Richard. 2010. “What Is APT and What Does It Want?” http://taosecurity.blogspot.cz/2010/01/what-is-apt-and-what-does-it-want.html

Bencsáth, Boldizsár, Pék, Gábor, Buttyán, Levente, and Márk Félegyházi. (2011). “Duqu:A Stuxnet-like malware found in the wild.” http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Benitez, Jorge, and Jason Healey. 2012. “Cybersecurity Pipe Dreams.” National Interest. http://nationalinterest.org/commentary/cyber-security-pipe-dreams-7254

Berger, Peter L, and Thomas Luckmann. 1966. "The Social Construction of Reality: A Treatise in the Sociology of Knowledge." New York. Vol. First Irvi.

Betz, David, and Tim Stevens. 2011. “Cyberspace and the State: Toward a Strategy for Cyber-Power.”

Betz, David. 2011. ‘Cyberwar’ is not coming. Infinity Journal, Issue 3 (Summer 2011): 21–24.

Beyer, Jessica L. 2014. “The Emergence of a Freedom of Information Movement.” Journal of Computer-Mediated Communication, Volume 19, Issue 2, pages 141–154, January 2014. http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12050/pdf

Bialik, Carl. 2013. “Putting a Price Tag on Film Piracy.” The Wall Street Journal, April 5. http://blogs.wsj.com/numbers/putting-a-price-tag-on-film-piracy-1228/

Bodmer, Sean, Kilger, Max, Carpenter, Gregory, and Jade Jones. 2012. "Reverse Deception: Organized Cyber Threat Counter-Exploitation." USA: McGraw-Hill.

Booth, Ken and Nicholas J. Wheeler. 2008. The Security Dilemma. "Fear, Cooperation and Trust in World Politics." New York: Palgrave Macmillan.

Boyle, James. 2003. “The Second Enclosure Movement and the Construction of the Public Domain.” Law and Contemporary Problems, Vol. 66, pp. 33-74, Winter-Spring 2003. http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1273&context=lcp

BSA. 2012. “Shadow Market.” BSA, The Software Alliance, May 2012. http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

BSA. 2014. “Compliance Gap.” BSA, The Software Alliance, June 2014. http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf

Budde. 2014. “Russia – Key statistics and Telecommunication Market.” http://www.budde.com.au/Research/Update-History.aspx?docid=2316

Bumiller, Elisabeth, and Thom Shanker. 2012. “Panetta Warns of Dire Threat of Cyberattack on US.” Online text: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Bussines Info. 2013. “Huawei fingered in Iranian sanction break.“ Bussiness Info, January 2. http://businesstech.co.za/news/electronics/29104/huawei-fingered-in-iranian-sanction-break/.

Cammaerts, Bart, Robin Mansell and Bingchun Meng. 2013. “Copyright & Creation.” The London School of Economics and Political Science, Media Policy Project, September 2013. http://www.lse.ac.uk/media@lse/documents/MPP/LSE-MPP-Policy-Brief-9-Copyright-and-Creation.pdf

Capoccia, Giovanni. 2000. “Defending democracy: Reactions to political extremism in inter-war Europe”, European Journal of Political research, 39, 4: 431-460. Netherlands, Kliwer Academic Publishers.

Casaretto, John. 2013. “NATO Document – Hacktivists Can Be Killer Under Rules of Cyber Warfare.” Silicon Angle, March 21st.

CCDCOE. 2013. "Tallinn Manual on the International Law Applicable to Cyber Warfare." Edited by Michael N. Schmitt. New York: Cambridge University Press.

Choucri, N. 2012. "Cyberpolitics in International Relations." MIT Press.

Christensen, T., J. 1999. "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia." International Security, 23:4.

Chrysopoulou, Eleni D. 2011. “The Budapest Convention as a Guarantee Limit Against Cybercrime.” Submitted to the 4th International Conference on Information Law, May 20-21, 2011. http://conferences.ionio.gr/icil2011/download.php?f=papers/055-chrysopoulou-full_text-en-v001.pdf

Clark, David, Diffie, Whitfield, and Abraham D. Sofaer. 2010. “Cyber Security and International Agreements.” Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. http://www.nap.edu/catalog.php?record_id=12997

Clark, Liat. 2012. “Pirate Bay traffic has doubled post-ISP blocks.” Wired, July 18. http://www.wired.co.uk/news/archive/2014-07/18/pirate-bay-traffic-doubles

Clarke, Richard A., and Robert K. Knake. 2010. “Cyberwar: The Next Threat to National Security and What to Do About It.” New York: Harper Collins.

Clayfield, Matthey. 2014. “Fillow Friday: @Kevin Rothrock explaining the RuNet.” Crikey. May 30. http://www.crikey.com.au/2014/05/30/follow-friday-kevinrothrock-explaining-the-runet/

Cloppert, Michael. 2009. “Security Intelligence: Introduction (pt1).” http://computer-forensics.sans.org/blog/2009/07/22/security-intelligence-introduction-pt-1

Command Five Pty Ltd. 2011.” Advanced Persistent Threats: A Decade in Review.” http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

Constitution of the Russian Federation. 1993. http://www.constitution.ru/

Convention on International Information Security. 2010. http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

Convention relative to the Treatment of Prisoners of War. 1949. Geneva.

Council of Europe. 2013. “Cybercrime. Action against economic crime.” http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

Council of Europe. 2001. "The Convention on Cybercrime." Budapest, November 23, 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

CPNI. 2005. “Targeted Trojan Email Attacks.” http://www.cpni.gov.uk/Documents/Publications/2005/2005015-BN0805_Targeted_trojan_email.pdf

Crawford, Timothy W. 2009. The Endurance of Extended Deterrence: Continuity, Change and Complexity in Theory and Policy. In: Complex Deterrence: Strategy in the Global Age, edited by Paul, Morgan, Wirtz, 277–303. Chicago, London: The University of Chicago Press.

Cri Online. 2013. “Huawei v ČR dynamicky roste a slaví již 10 let působení na českém trhu.“ November 21. http://czech.cri.cn/719/2013/11/21/1s145900.htm.

Criminal Code of the Russian Federation. 1996. http://www.rg.ru/2007/11/12/ukrf-dok.html

Crouch, Erik. 2013. “Huawei CEO Ren Zhengfei just gave one of the weirdest interviews ever.“ Shanghaiist, December 10. ttp://shanghaiist.com/2013/12/10/huawei_ceo_ren_zhengfei_just_gave_o.php.

CrySyS. 2012. „sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks.“ http://www.crysys.hu/skywiper/skywiper.pdf

Cybersecurity News. 2012. “UN Criticizes Iran’s Cybersecurity Strategy.” http://cybersecuritynews.org/2012/10/29/un-criticizes-irans-cybersecurity-strategy/

Dahl, R. Alan. 1971. "Polyarchy: Participation and Opposition." Yale University Press.

Dam, Kenneth, W., Lin, Herbert, S., and William A.Owens (eds.). 2009. “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.” Committee on Offensive Information Warfare, National Research Council. http://www3.nd.edu/~cpence/eewt/Owens2009.pdf

Danaher, Brett, and Joel Waldfogel. 2012. “Reel Piracy: The Effect of Online Film Piracy on International Box Office Sales.” Social Science Research Network, January 16. http://ssrn.com/abstract=1986299

Davidoff, Victor. 2014. “An Internet Censorship Law Right Out of 1984.” The Moscow Times. April 27. http://www.themoscowtimes.com/opinion/article/an-internet-censorship-law-right-out-of-1984/498982.html

Defense Tech. 2010. “Israel Adds Cyber-Attack to IDF.” http://defensetech.org/2010/02/11/israel-adds-cyber-attack-to-idf/.

Demchak, Chris C. 2011. Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security. Athens, GA: University of Georgia Press. Online: Ebrary.

Demchak, Chris C., and – Peter Dombrowski. 2011. Rise of a Cybered Westphalian Age. Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011): 32–61. Online: http://www.au.af.mil/au/ssq/spring11.asp.

Denning, Dorothy E. 1998. "Information Warfare and Security". Addison-Wesley Professional; 1 edition.

Department of Business Innovation and Skills. "Call of Evidence for Proposed EU Directive on Network and Information Security: Summary of Responses," September 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/237069/bis-13-1169-call-for-evidence-on-proposed-eu-directive-on-network-and-information-security.pdf

Deterrence. 2012. "DOD Dictionary of Military Terms." Joint Education and Doctrine Division, J–7. Department of Defense. Online: http://www.dtic.mil/doctrine/dod_dictionary/data/d/3763.html.

Diamond, Larry and Juan J. Linz and Seymour Martin Lipset, eds. 1988." Democracy in Developing Countries: Asia, Africa, and Latin America." Boulder: Lynne Rienner Publishers.

Digital Trends. 2013. "To Russian with Internet Restrictions is Moscows Anti-child Porn Plan Good Sense or Censorship." http://www.digitaltrends.com/social-media/to-russia-with-internet-restrictions-is-moscows anti-child-porn-plan-good-sense-or-censorship/

Dinstein, Yoram. 2012. "The Principle of Distinction and Cyber War in International Armed Conflicts." Journal of Conflict & Security Law 17, 2: 261-277.

DoS. 2013. "Country Reports on Terrorism 2012." http://www.state.gov/documents/organization/210204.pdf

Downing, Richard. "Legal frameworks to Combat Cybercrime – An Overview of Efforts in Asia-Pacific." Presentation for the 14th session. http://www.itu.int/osg/spu/cybersecurity/presentations/session14_downing.pdf

Doyle, James H. 2002. "Compuer Networks, Proportionality, and Military Operations." In Computer Network Attack and International Law, edited by Michael N. Schmitt and Brian T. O'Donnell, 147-161. Newport, R. I.: Naval War College.

Droege, Cordula. 2012. "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians". International Review of the Red Cross 94, 886: 533-578.

Dunn Cavelty, Myriam. 2014. "Breaking the Cyber Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." Science and Engineering Ethics. https://www.academia.edu/6960037/Breaking_the_Cyber-Security_Dilemma_Aligning_Security_Needs_and_Removing_Vulnerabilities

Dunn, John E. 2014. "Invisible Russian cyberweapon stalked US and Ukraine since 2005, new research reveals." http://news.techworld.com/security/3505688/invisible-russian-cyberweapon-stalked-us-and-ukraine-since-2005-new-research-reveals/

Elder, Miriam. 2012. "Hacked E-mails allege Russian youth group Nashi Paying Bloggers." The Guardian. February 7. http://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers

Elwell, Andrew. 2013. “UK first to admit developing cyber offensive capabilities.” http://www.defenceiq.com/cyber-defence/articles/game-changer-uk-first-to-admit-to-developing-cyber/.

EMC. 2014. “RSA SecurID.” http://www.emc.com/security/rsa-securid.htm

Enigmax. 2012. “Pirate Bay Enjoys 12 Million Traffic Boost, Shares Unblocking Tips.” TorrentFreak, May 2. https://torrentfreak.com/pirate-bay-enjoys-12-million-traffic-boost-shares-unblocking-tips-120502/

Enigmax, Ernesto. 2011. “Swiss Govt: Downloading Movies and Music Will Stay Legal.” TorrentFreak, December 2. https://torrentfreak.com/swiss-govt-downloading-movies-and-music-will-stay-legal-111202/

Eritrea Ethiopia Claims Commission. 2005. Partial Award – Western Front, Aerial Bombardment and Related Claims. Hague.

Ernesto. 2010. “Behind the Scenes at Anonymous Operation Payback.” TorrentFreak, November 15. https://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015/

Ernesto. 2014. “Game of Thrones Finale Sets New Piracy Record.” TorrentFreak, June 16. http://torrentfreak.com/game-thrones-season-finale-sets-piracy-record-140616/

Ertuna, Irmak. 2009. “Digital Pirates and the Enclosure of the Intellect.” Darkmatter Journal, December 20. http://www.darkmatter101.org/site/wp-content/uploads/pdf/5_Ertuna_Pirates_and_Piracy.pdf

Essers, Loek. 2014. “Dutch court ends Pirate Bay blockade after digital piracy continued to thrive.” PCWorld, January 28. http://www.pcworld.com/article/2092040/dutch-court-finds-pirate-bay-block-ineffective-ends-it.html

EU. 2013. “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”. Brussels. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

European Union Agency for Network and Information Security. “Mission.” http://www.enisa.europa.eu/about-enisa/activities/mission

Fairlie, Simon. 2009. “A Short History of Enclosure in Britain.” The Land, Issue 7, Summer 2009. http://www.thelandmagazine.org.uk/articles/short-history-enclosure-britain

Fawcett, Lousie. 2004. “Exploring Regional Domains: A Comparative History of Regionalism.” International Affairs 80:3: 429-446. http://www.chathamhouse.org/sites/default/files/public/International%20Affairs/Blanket%20File%20Import/inta_391.pdf

Federal Ministry of Defence of the Federal Republic of Germany. Humanitarian Law in Armed Conflicts – Manual. 1992.

Ferro, Greg. 2012. “The Huawei Security Problem Isn’t the Hardware, it’s Engineers Fixing the Bugs.“ Etherealmind, October 29. http://etherealmind.com/the-huawei-security-problem-isnt-the-hardware-its-engineers-fixing-the-bugs/

Finkle, Jim. 2013. “Microsoft, FBI take aim at global cyber crime ring.” Reuters, June 5. http://www.reuters.com/article/2013/06/05/net-us-citadel-botnet-idUSBRE9541KO20130605

Finnemore, Martha, and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change.” International Organization 52: 4: 887-917

Ford, Christopher, A. 2010. “The Trouble with Cyber Arms Control.” The New Atlantis 29. http://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control

Forum of Incident Response and Security Teams. “Members around the World. http://www.first.org/members/map

Freedom House. 2014a. “Freedom in the World: Russia – 2014 Scores.” https://freedomhouse.org/report/freedom-world/2014/russia#.VQx2O46G93Q

Freedom House. 2014b. “Freedom on the Net: Russia.” https://freedomhouse.org/report/freedom-net/2014/russia

Freedom House. 2015. “Freedom in the World: Russia – 2015 Scores.” https://freedomhouse.org/report/freedom-world/2015/russia#.VQx2-46G93Q

G Data. 2014. “Uroburos.” https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

Gantz, John F., Alejandro Florean, Richard Lee, Victor Lim, Biplab Sikdar, Sravana Kumar Sristi Lakshmi, Logesh Madhavan and Mangalam Nagappan. “The Link between Pirated Software and Cybersecurity Breaches.” IDC, National University of Singapore, Microsoft, March 2014. http://www.microsoft.com/en-us/news/downloads/presskits/dcu/docs/idc_031814.pdf

GAO. 2010. “Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods.” Government Accountability Office, April 12. http://www.gao.gov/assets/310/303057.pdf

Garden, Timothy. 2002. "Air Power: Theory and Practice." In: Strategy in the Contemporary World: An Introduction to the Strategic Studies, edited by Baylis, Wirtz, Cohen, and Gray, 137–157. New York: Oxford University Press, First Edition.

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” International Security 38 (2): 41–73. http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf

Gasudarsvjenaja Duma. 2013. „Zakonaprajekt № 89417-6. http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=89417-6)

Geers, Kenneth. 2011. “Strategic Cyber Security.” Tallinn: NATO CCD COE Publication.

Gertz, Bill. 2011. “Chinese telecom firm tied to spy ministry.“ The Washington Times, October 11. http://www.washingtontimes.com/news/2011/oct/11/chinese-telecom-firm-tied-to-spy-ministry/?page=all.

Gibson, William. 1984. "Neuromancer." Ace Books.

Giddens, Anthony. 1979. "Central Problems in Social Theory."

Gilbert, Leah and Mohseni, Payam. 2011. Beyond Authoritarianism: The Conceptualization of Hyberid Regimes. Springer Science+Business Media.
http://dingo.sbs.arizona.edu/~ggoertz/pol682qm/Gilbert_Mohseni2011.pdf

Giles, Keir. 2012. "Russias Public Stance on Cyberspace Issues." CCDCOE, NATO.
https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf

Gonsalves, Chris. 2014. "Huawei Ready for an American Do-over." Channelnomics, April 4.
http://channelnomics.com/2014/04/04/huawei-ready-american/.

Google. 2010. „A new approach to China." http://googleblog.blogspot.cz/2010/01/new-approach-to-china.html

Gostev, Alexander. 2012a. "The Flame: Questions and Answers."
http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

Gostev, Alexander. 2012b. "The Mystery of Duqu: Part Ten."
http://www.securelist.com/en/blog/208193425/The_mystery_of_Duqu_Part_Ten

Gostev, Alexander. 2014. "Agent.btz: a Source of Inspiration?"
http://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/

Gragido, Will. 2012. "Lions at the Watering Hole – The 'VOHO' Affair.".
http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/

Grasso, Giancarlo. 2009. "The Role of Europe in Matching Today's Asymmetric Threats." In Modelling Cyber Security: Approaches, Methodology, Strategies, edited by U. Gori. IOS Press.

GReAT. 2012a. "Gauss: Nation-state cyber-surveillance meets banking Trojan."
http://securelist.com/blog/incidents/33854/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/

GReAT. 2012b. "Gauss: Abnormal Distribution." http://securelist.com/analysis/36620/gauss-abnormal-distribution/

GReAT. 2013a. "'Red October' Diplomatic Cyber Attacks Investigation."
http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/

GReAT. 2013b. "'Red October'. Detailed Malware Description 1. First Stage of Attack."
http://securelist.com/analysis/publications/36830/red-october-detailed-malware-description-1-first-stage-of-attack/

GReAT. 2013c. "The Icefog APT: Frequently Asked Questions."
http://securelist.com/analysis/publications/57892/the-icefog-apt-frequently-asked-questions/

GReAT. 2014a. The Careto/Mask APT: Frequently Asked Questions.
http://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/

GReAT. 2014b. "The Epic Turla Operation." http://securelist.com/analysis/publications/65545/the-epic-turla-operation/

GReAT. 2014c. "'El Machete'." http://securelist.com/blog/research/66108/el-machete/

Greene, Tim. 2012. "How Microsoft is taking down Nitol botnet." TechWorld, September 17. http://features.techworld.com/security/3381643/in-depth-how-microsoft-is-taking-down-nitol-botnet/

Grossman, Elaine M. 2009. "U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack." http://www.nti.org/gsn/article/us-general-reserves-right-to-use-force-even-nuclear-in-response-to-cyber-attack/.

Guitton, Clement, and Elaine Korzak. 2013. "The Sophistication Criterion for Attribution." RUSI Journal 158:62-68. doi: 10.1080/03071847.2013.826509

Haggard, Stephan, and Beth A. Simons. 1987 "Theories of International Regimes." International Organization 41:3. http://www.jstor.org/stable/2706754

Hague Rules of Air Warfare. 1923. Hague.

Harper, Jim. 2010. "Fact-Checking „Cyberwar"." http://www.cato.org/blog/fact-checking-cyberwar

Hawes, John. 2014. "Anti-piracy group warns about malware-riddled sites - fair, or scaremongering?" Naked Security, Sophos, May 2. http://nakedsecurity.sophos.com/2014/05/02/anti-piracy-group-warns-about-malware-riddled-sites-fair-or-scaremongering/

Heickerö, Roland. 2010. "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations." Stockholm: FOI.

Heinl, Caitriona, H. 2013. "Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime," S. Rajaratnam School of International Studies. https://dr.ntu.edu.sg/bitstream/handle/10220/20057/WP263.pdf?sequence=1

Hernandez-Ardieta, Jorge, L., Suarez-Tangli, Guillermo, and Juan E. Taplador. 2013. "Information Sharing Models for Cooperative Cyber Defence." In The 5th International Conference on Cyber Conflict. Maybaum, M., Podins, K., Stinissen, J. (Eds.). Tallinn: NATO CCD COE Publications, 2013. http://www.ccdcoe.org/publications/2013proceedings/d1r2s2_hernandezardieta.pdf

Herz, J., H. 1950. "Idealist Internationalism and the Security Dilemma." World Politics. 2:2: 157-180. http://www.jstor.org/stable/2009

Hibberd, James. 2013. "HBO: 'Game of Thrones' piracy is a compliment." Entertainment Weekly, March 31. http://insidetv.ew.com/2013/03/31/hbo-thrones-piracy/

Higgins, Kelly J. 2013. "'Red October' Attacks: The New Face of Cyberespionage." http://www.darkreading.com/attacks-breaches/red-october-attacks-the-new-face-of-cyberespionage/d/d-id/1138972?

Hill, Brandon. 2014. "Report: NSA Has Been Spying on Huawei Networking Equipment, Execs Since 2007". Dailytech, March 23. http://www.dailytech.com/Report+NSA+Has+Been+Spying+on+Huawei+Networking+Equipment+Execs+Since+2007/article34571.htm

Hloušek, Vít, and Lubomír Kopeček, eds. 2007. "Demokracie. Teorie, modely, osobnost, podmínky, nepřátelé a perspektivy demokracie." Brno: Mezinárodní politologický ústav Masarykovy univerzity.

Hloušek, Vít, Kopeček, Lubomír, and Jakub Šedo, eds. 2011. "Politické systémy." Brno: Barrister & Principal.

Hollis, Martin, and Steve Smith. 1990. Explaining and Understanding International Relations. Oxford: Clarendon Press.

Human Rights Watch. 2013. "Human Rights Watch Daly Brief, 22 November." http://www.hrw.org/news/2013/11/22/human-rights-watch-daily-brief-22-november

Huawei. 2014a. "Products." http://enterprise.huawei.com/en/products/index.htm?navi=0.

Huawei. 2014b. "Index." http://enterprise.huawei.com/en/index.htm.

Huyghe, François-Bernard. 2011. "Cyberwar and its Borders." In: Ventre, Daniel (ed.): Cyberwar and Information Warfare. London: ISTE.

IbnLive. 2013."Huawei founder Ren Zhengfei gives first ever media interview." 2013. IbnLive, May 10 http://ibnlive.in.com/news/huawei-founder-ren-zhengfei-gives-first-ever-media-interview/390798-11.html

IFPI. 2004. "Serious, VIolent and Organised Crime." International Federation of the Phonographic Industry, 2004. http://www.ifpi.org/content/library/music-piracy-organised-crime.pdf

IfsecGlobal. 2010. "Huawei eyes security evaluation unit in India." 2010. IfsecGlobal, December 31. http://www.ifsecglobal.com/huawei-eyes-security-evaluation-unit-in-india/

Ihned. 2013. "Rusko za necelé dva týdny cenzury zablokovalo skoro 200 webových stránek." http://zahranicni.ihned.cz/c1-58452890-rusko-cenzura-web-internet

Ihned. 2013b. "Rusko zavádí černý seznam nežádoucích webů. Opozice se bojí cenzury." http://zahranicni.ihned.cz/c1-58193560-rusko-zavadi-cerny-seznam-nezadoucich-webu-opozice-se-boji-cenzury

Infosecurity Magazine. 2013. "Kimsuky – an active North Korean campaign targeting South Korea." http://www.infosecurity-magazine.com/news/kimsuky-an-active-north-korean-campaign-targeting/

Intelligence and Security Committe. 2013. "Foreign involvement in the Critical National Infrastructure: The implications for national security." Norwich: TSO (The Stationery Office). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf

International Court of Justice. Legality of the threat or use of nuclear weapons: Advisory Opinion of 8 July 1996.

International Criminal Tribunal for the former Yugoslavia. Prosecutor v. Stanislav Galić, Judgement and Opinion of 5 December 2003.

International Criminal Tribunal for the former Yugoslavia. Prosecutor v. Tadić. Opinion and Judgment of 7 May 1997.

Isidore, Chris. 2013. “Game of Thrones premiere sets piracy record.” CNN Money, April 2. http://money.cnn.com/2013/04/02/technology/game-of-thrones-piracy/

ITAR-TASS. 2014. “Kommersant Publishers Call to Sue prp-Kremlin Nashi Movement.” http://tass.ru/en/archive/669564

Jensen, Eric Talbot. 2003. “Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?” American University International Law Review 18, 5: 1145-1188.

Jervis, Robert. 1978. “Cooperation under the Security Dilemma.” World Politics 30(2): 167–214

Johns, Adrian. 2013. Pirátství. Brno: Host, 2013.

Joint Staff. 2013. “Joint Pub 3-27: Homeland Defense”. http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf

Jones, Ben. 2009. “MPAA Study Links Piracy to Gangs and Terrorists.” TorrentFreak, March 4. https://torrentfreak.com/mpaa-study-links-film-piracy-to-gangs-and-terrorists-090304/

Kain, Roger J. P., John Chapman and Richard R. Oliver. 2004. “The enclosure movement in England and Wales.” Cambridge University Press, July 2004. http://assets.cambridge.org/97805218/27713/excerpt/9780521827713_excerpt.pdf

de Kaminski, Marcin. 2013. “The Survey Bay, a searchable database covering the Pirate Bay community.” Cybernormer, August 29. http://cybernormer.se/the-survey-bay-a-searchable-database-covering-the-pirate-bay-community/

Kaminski, Ryan, T. 2010. “Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions.” In Conference on Cyber Conflict, Proceedings 2010. Czosseck, C., and K. Podins. (eds.). Tallinn: NATO CCD COE Publications. http://www.ccdcoe.org/publications/2010proceedings/Kaminski%20-%20Escaping%20the%20Cyber%20State%20of%20Nature%20Cyber%20deterrence%20and%20International%20Institutions.pdf

Kamluk, Vitaly, Soumenkov, Igor, and Costin Raiu. 2014. “The Icefog APT Hits US Targets With Java Backdoor.” http://securelist.com/blog/incidents/58209/the-icefog-apt-hits-us-targets-with-java-backdoor/

Kan, Michael. 2011. “China's Huawei reveals board members to boost transparency.“ Goodgearguide, April 18. http://www.pcworld.idg.com.au/article/383594/china_huawei_reveals_board_members_boost_transparency/.

Kan, Michael. 2013. “UK to probe Huawei's cybersecurity evaluation center.“ Techworld, July 19. http://news.techworld.com/security/3459688/uk-to-probe-huaweis-cybersecurity-evaluation-center/.

Karaganis, Joe. 2010. “Piracy and Jobs in Europe.” Social Science Research Council, December 2010. http://piracy.americanassembly.org/wp-content/uploads/2010/12/Piracy-and-Jobs-in-Europe-a-note-on-the-BASCAP-TERA-study.pdf

Karaganis, Joe, Pedro Mizukami, Lawrence Liang, John Cross and Olga Sezneva. 2011. “Does Crime Pay? MPEE’s Findings on Piracy, Organized Crime, and Terrorism.” Social Science Research Council, February 2011. http://piracy.americanassembly.org/wp-content/uploads/2011/02/Does-Crime-Pay.pdf

Karl, L. Terry. 2005. "The Hybrid Regimes of Central America." Journal of Democracy, 6, 3.

Kaspersky. 2010. “Stuxnet Worm: Insight from Kaspersky Lab.” http://www.kaspersky.com/about/news/virus/2010/Stuxnet_Worm_Insight_from_Kaspersky_Lab

Kaspersky. 2012. “Kaspersky Lab Discovers ‘Gauss¨- A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts.” http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

Kaspersky. 2013a. ”Flame.” http://www.kaspersky.com/flame

Kaspersky. 2013b. “Kaspersky Lab Exposes Icefog. A New Cyber-espionage Campaign Focusing on Supply Chain Attacks.” http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

Kaspersky. 2013c. “Kaspersky Lab Analyzes Active Cyber-Espionage Campaign Targeting South Korean Entities.” http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Analyzes_Active_Cyber-Espionage_Campaign_Primarily_Targeting_South_Korean_Entities

Kaspersky. 2014a. “Unveiling ‘Careto’ – The Masked APT.” http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

Kaspersky. 2014b. “How Turla and ‘worst breach of U.S. military computers in history’ are connected.” http://www.kaspersky.com/about/news/virus/2014/How-Turla-and-worst-breach-of-US-military-computers-in-history-are-connected

Kelsey, Jeffrey T. G. 2008. “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.” Michigan Law Review 106, 7: 1427-1452.

Kerr, Dara. 2012. “Pirate Bay ditches servers and switches to the cloud.” CNET, October 17. http://www.cnet.com/news/pirate-bay-ditches-servers-and-switches-to-the-cloud/

Kramer, Franklin D. 2009. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In: Cyberpower and National Security, edited by Kramer, Starr, and Wentz, 3–23. Washington D.C.: National Defense University Press; Potomac Books.

Krepinevich, Andrew. 2012. "Cyber Warfare: A Nuclear Option?" Washington D.C.: Center for Strategic and Budgetary Assessments (CSBA). Online: http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In: Cyberpower and National Security, edited by Kramer, Starr, and Wentz, 24–42. Washington D.C.: National Defense University Press; Potomac Books.

Kugler, Richard L. 2009. "Deterrence of Cyber Attacks." In: Cyberpower and National Security, edited by Kramer, Starr, and Wentz, 309−340. Washington D.C.: National Defense University Press; Potomac Books.

Langner, Ralph. 2013. “To Kill a Centrifuge. A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Latour, Bruno. 1996. "Aramis or the Love of Technology." London: Harvard University Press.

Leadership. 2012. “Huawei Launches Intelligent Railway Solution.“ September 27. http://www.leadershiponline.co.za/articles/huawei-launches-intelligent-railway-solution-2328.html.

Leciánová, Alena. 2013. “Advanced Persistent Threat: koncept, případy a kritéria.” Bachelor thesis. Masaryk University.

Lee, John. 2012. “The other side of Huawei.“ BusinessSpectator, April 30. http://www.businessspectator.com.au/article/2012/3/30/australian-news/other-side-huawei.

Legro, Jeffrey W. 1997. “Which Norms Matter? Revisiting the ‘Failure’ of Internationalism.” International Organization 51:1: 31-63

Lettice, John. 2004. “Piracy funds terror, Guardian lesson tells schools.” The Register, November 17. http://www.theregister.co.uk/2004/11/17/graun_piracy_lessons/

Lewis, James A. 2002. “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lewis, James A. 2009. “The "Korean" Cyber Attacks and Their Implications for Cyber Conflict.” Center for Strategic and International Studies. http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf

Libicki, Martin. 2007. "Conquest in Cyberspace: National Security and Information Warfare." Cambridge University Press.

Libicki, Martin. 2009. "Cyberdeterrence and cyberwar**Error! Bookmark not defined.**." RAND Project Air Force. Rand Corporation. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, Martin. 2013. “Don’t Buy the Cyberhype: How to Prevent Cyberwars From Becoming Real Ones.” http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype.

Lin, Herbert. 2012. “Cyber conflict and international humanitarian law.” International Review of the Red Cross 94, 886: 515-531.

Linz, J. Juan. 1975. “Totalitarian and authoritarian regimes.” In: Handbook of political science, vol. 3. Eds. Greenstein, I. Fred. and Polsby, W. Nelson. Reading MA: Addison-Wesley.

LiveMint. 2014. “Huawei allegedly hacked BSNL network: govt.“ February 5. http://www.livemint.com/Industry/L0YQ5YUMWkDcyDsrMTFQwJ/Huawei-allegedly-hacked-BSNL-network-govt.html.

Lockheed Martin. 2011. “Lockheed Martin Customer, Program and Employee Data Secure.” Accessed http://www.lockheedmartin.com/us/news/press-releases/2011/may/LockheedMartinCustomerPro.html

Loewenstein, Karl. 1937a. “Legislative Control of Political Extremism in European Democracies I.” Columbia Law Review, 38, 4.

Loewenstein, Karl. 1937b. “Legislative Control of Political Extremism in European Democracies II.” Columbia Law Review, 38, 5.

Loewenstein, Karl. 1938a. “Militant Democracy and Fundamental Rights I.” The American Political Science Review, 31, 3.

Loewenstein, Karl. 1938b. “Militant Democracy and Fundamental Rights II.” The American Political Science Review, 31, 4.

Lonsdale, David J. 2003. "Information Power: Strategy, Geopolitics and the Fifth Dimension." In: Geopolitics: Geography and Strategy, edited by Gray and Sloan, 137–157. London, Portland: Frank Cass Publishers.

Lynn, William J. 2010. “Defending a New Domain: The Pentagon’s Cyberstrategy.” In: Foreign Affairs, vol. 85, No. 5: 97-108.

Maďar, Tomáš, and Tomáš Rezek. 2014. “Prague Transatlantic Talks 2014: Facing the Atlantic Cyber Challenge. Conference Report 4/2014.” http://www.amo.cz/publikace/prague-transatlantic-talks-2014-facing-the-atlantic-cyber-challenge-2.html.

Mahnken, Thomas G. 2011. "Cyber war and cyber warfare." In: America’s Cyber Future: Security and Prosperity in the Information Age, Volume II., edited by Lord and Sharps, 55–64. Center for a New American Security. Online: http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf.

Maltman, Stuart. 2013. “Securitization Theory and the Limits of Security Studies.” The Ethics of Security and the Ethics of Securitization, BISA Conference, Birmingham, 2013. http://bisa.ac.uk/index.php?option=com_bisa&task=download_paper&no_html=1&passed_paper_id=360

Mandiant. 2013. “APT1: Exposing One of China’s Cyber Espionage Units.” http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Manness Ryan C., and Brandon Valeriano. 2014. “The dynamics of cyber conflict between rival antagonists, 2001−11.” Journal of Peace Research 51:3: 347-360. http://jpr.sagepub.com/content/51/3/347

Mareš, Miroslav, 2007. “Polyarchie.” In: Demokracie. Teorie, modely, osobnost, podmínky, nepřátelé a perspektivy demokracie. Eds. Hloušek, Vít a Kopeček, Lubomír. Brno: Mezinárodní politologický ústav Masarykovy univerzity.

Marion, Nancy E. 2010. “The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation.” International journal of Cyber Criminology 4: 1 and 2. http://www.cybercrimejournal.com/marion2010ijcc.pdf

Masnick, Mike. 2013. “Piracy Doesn't Create A Loss To 'The Economy,' But To A Particular Industry.” TechDirt, August 2. https://www.techdirt.com/articles/20130727/02110623966/piracy-doesnt-create-loss-to-economy-to-particular-industry.shtml

McAfee. 2011. “Global Energy Cyberattacks: ‘Night Dragon’.” http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

McAfee. 2014. ”Careto Attack – The Mask.” https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25037/en_US/McAfee_Labs_Threat_Advisory_Careto_Attack_The%20Mask_3.pdf

McAllister, Neil. 2013. “Surprised? Old Java exploit helped spread Red October spyware.” Accessed http://www.theregister.co.uk/2013/01/16/red_october_java_connection/

McCullagh, Declan. 2005. “Terrorist link to copyright piracy alleged.” CNET, May 27. http://news.cnet.com/Terrorist-link-to-copyright-piracy-alleged/2100-1028_3-5722835.html

McGraw, Gary. 2013. “Cyber War Is Inevitable (Unless We Build Security In).” Journal of Strategic Studies 36 (February): 109–119.

McLuhan, M. 1990. “The Road to the Global Village.” Scientific American 262: 83–94.

McQuade, Samuel C., ed. 2009. "Encyclopedia of Cybercrime." Connecticut: Greenwood Press.

Melzer, Nils. 2009. Interpretative Guidance on the notion of direct participation in hostilities under international humanitarian law. Geneva: ICRC.

Meyer, David. 2012. “Pirate Bay abandons torrent file links for Magnets.” ZDNet, February 29. http://www.zdnet.com/pirate-bay-abandons-torrent-file-links-for-magnets-4010025519/

Michael, Peter. 2003. “Huawei 'broke Iraq embargo'.“ South China Morning post, March 23. http://www.scmp.com/article/410267/huawei-broke-iraq-embargo.

Morris, Anne. 2013. “Huawei wins TDC LTE deal away from Ericsson.“ Fierce Wireless, September 18. http://www.fiercewireless.com/europe/story/huawei-wins-tdc-lte-deal-away-ericsson/2013-09-18.

Mueller, John. 1991. “Pearl Harbor. Military Inconvenience, Political Disaster.” In: International Security, vol. 16, No. 3, 172-203.

Mueller, John, and Benjamin Friedman. 2013. “The Cyberskeptics.” http://www.cato.org/research/cyberskeptics.

Nagaraja, Shishir, and Ross Anderson. 2009. “The snooping dragon: social-malware surveillance of the Tibetan movement.” http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf

Nakamoto, Satoshi. 2008. “Bitcoin : A Peer-to-Peer Electronic Cash System”: 1–9. https://bitcoin.org/bitcoin.pdf

National Security Agency. 2013. “Computer Network Operations.” http://www.nsa.gov/careers/career_fields/netopps.shtml.

National Research Council. 2009. "Cyberattack Capabilities." National Academy Press. Washington, D.C.: National Academy Press.

National Research Council. 1999. "Realizing the Potential of C4I: Fundamental Challenges." Computer Science and Telecommunications Board, Washington, D.C.: National Academy Press.

NATO. 2014. „What is SHAPE?“ http://www.aco.nato.int/shape.aspx

Newsweek. 1999. “’We’re In The Middle Of A Cyberwar‘.” Updated March 14, 2010. http://www.newsweek.com/were-middle-cyerwar-166196

Oberholzer-Gee, Felix, and Koleman Strumpf. 2010. “File-Sharing and Copyright.” Music Business Research, January 12, 2010. http://musicbusinessresearch.files.wordpress.com/2010/06/paper-felix-oberholzer-gee.pdf

O’Donnell, Brian T. and Kraska, James. 2003. “Humanitarian Law: Developing International Rules for the Digital Battlefield.” Journal of Conflict & Security Law 8, 1: 133-160.

OECD. 2008. “The Economic Impact of Counterfeiting and Piracy.” Structural Policy Division of the OECD Directorate for Science, Technology and Industry, 2008. http://www.oepm.es/cs/OEPMSite/contenidos/ponen/InformeOCDE26feb09/2009_03_03_OECD_Study_on_Counterfeiting_and_Piracy.pdf

Opennet Initiative. 2010. “Russia.” https://opennet.net/research/profiles/russia

Parks, W. Hays. 1990. “Air War and the Law of War.” Air Force Law Review 32, 1: 1-225.

Parland, Thomas. 2005. "The Extreme Nacionalist Threat In Russia: The Growing Influence of Western Ideas." London – New Yoirk: Routledge Curzon.

Paul, T. V. 2009. "Complex Deterrence: An Introduction." In: Complex Deterrence: Strategy in the Global Age, edited by Paul, Morgan, and Wirtz, 1–27. Chicago, London: The University of Chicago Press.

Payne, Keith B. 2001. "The Fallacies of Cold War Deterrence and a New Direction." [s.l.]: The University of Kentucky Press.

Payne, Keith B. 2008. "The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century." Fairfax: National Institute Press.

Payne, Keith. B., and Walton, C. Dale. 2002. "Deterrence in the Post-Cold War World." In: Strategy in the Contemporary World: An Introduction to the Strategic Studies, edited by Baylis, Wirtz, Cohen, and Gray, 161–182. New York: Oxford University Press, First Edition.

Phersmann, Otto. 2004. In: Thiel, Marcus. 2009. "The Militant democracy principle in Modern Democracies." Farnham: Ashgate.

Piraty party. 2014. “Federal Law N 139-ФЗ and legislative measure 89417-6 2012.“. http://pirate-party.ru/content/с-новым-годом-усиления-цензуры

Plassaras, Nicholas A. 2013. “Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF.” Chicago Journal of International Law 14: 377–407.

Poort, Joost, and Jorna Leenheer. 2012. “File sharing 2©12.” Institute for Information Law, November 30. http://www.ivir.nl/publications/poort/Filesharing_2012.pdf

Poort, Joost, Jorna Leenheer, Jeroen van der Ham and Cosmin Dumitru. 2013. “Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay.” Institute for Information Law, August 22. http://www.ivir.nl/publications/poort/Baywatch.pdf

Prasso, Sheridan. 2011. “What makes China telecom Huawei so scary?“ Fortune, July 28. http://fortune.com/2011/07/28/what-makes-china-telecom-huawei-so-scary/.

Prolexic. 2012. “Prolexic Quarterly Global DDoS Attack Report.” http://www.preventia.co.uk/resources/data_sheets/prolexic/Prolexic_Quarterly_Global_DDoS_Attack_Report_Q412_A4_011413-1.pdf

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts. Geneva, 1977.

Radware. 2014. Command and Control Server.” http://security.radware.com/knowledge-center/DDoSPedia/command-and-control-server/

Rashid, Fahmida, Y. 2013. “Microsoft Compares Malware Infection Rates, Socio-Economic Factors.” Security Watch. http://securitywatch.pcmag.com/microsoft/307922-microsoft-compares-malware-infection-rates-socio-economic-factors

Rattray, Gregory J. 2009. "An Environmental Approach to Understanding Cyberpower." In: Cyberpower and National Security, edited by Kramer, Starr, and Wentz, 253–274. Washington D.C.: National Defense University Press; Potomac Books.

Reed, John. 2013. “Africa's Big Brother Lives in Beijing.“ Foreing policy, July 30. http://www.foreignpolicy.com/articles/2013/07/30/africas_big_brother_lives_in_beijing_huawei_china_surveillance.

Rejaie, Reza, Michal Kryczka, Roberto Gonzalez, and Noel Crespi. “Investigating the Reaction of BitTorrent Content Publishers to Antipiracy Actions.” http://mirage.cs.uoregon.edu/pub/antipiracy-IEEE_P2P_v10.pdf

Reporters Without Borders. 2012. “Internet Enemies report 2012.” World Day Against Cyber Censorship. http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf

RIA Novosti, 2012. “Russian Internet Blacklist 96 % Illegal – Pirates.” http://en.ria.ru/russia/20121217/178221958.html

RIA Novosti. 2013a. “Petition Against Russian Anti-piracy Law Gets 100000 Signatures Online.” http://en.ria.ru/russia/20130810/182696433/Petition-Against-Russian-Anti-piracy-Law-Gets-100000-Signatures-Online.html

RIA Novosti 2013b “Russia ti Block First Webside Under Piracy Law.” http://en.ria.ru/crime/20130821/182888505/Russia-to-Block-First-Website-Under-Anti-Piracy-Law.html

Rid, Thomas. 2012a. "What War in the Fifth Domain." Kings of War (Department of War Studies, King's College London, August 9, 2012. Online: http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/.

Rid, Thomas. 2013. "Cyberwar Will Not Take Place." London: Hurst.

Roberts, Dexter. 2012. "Huawei, ZTE, and Chinese Investment in the U.S." Businessweek, October 8. http://www.businessweek.com/articles/2012-10-08/huawei-zte-and-chinese-investment-in-the-u-dot-s-dot

Roberts, Hal, and Bruce Etling. 2011. "Coordinated DDoS Attack During Russian Duma Elections". Internet & Democracy blog. http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/

Robertson, Adi. 2014. "Putin Sings Law Forcing Bloggers to register Blobbers with Russian Media Office." The Verge. http://www.theverge.com/2014/5/7/5690410/putin-signs-law-forcing-bloggers-to-register-with-russian-media-office

Rollins, John and Liana Sun Wyler. 2013. "Terrorism and Transnational Crime: Foreign Policy Issues for Congress." http://www. http://fas.org/sgp/crs/terror/R41004.pdf

Ross, Nick. 2011. "The case for piracy." ABC - Technology, October 21. http://www.abc.net.au/technology/articles/2011/10/20/3344351.htm

Ross, Nick. 2014. "Game of Thrones and the case for piracy." ABC - The Drum, April 9. http://www.abc.net.au/news/2014-04-08/ross-game-of-thrones-and-the-case-for-piracy/5375758

Rothrock, Kevin. 2014. "Andrey Mima on banning the Internet in Russia." The Global Voices. http://globalvoicesonline.org/2014/07/04/russia-censorship-internet-servers-law-mima/

RSA. 2011. "Anatomy of an Attack." https://blogs.rsa.com/anatomy-of-an-attack/

Rueter, Nicholas C. 2011. "The Cybersecurity Dilemma." Master Thesis, Duke Unversity. http://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/3793/Rueter_duke_0066N_10959.pdf%3Fsequence%3D1

Rutland, Peter. 2008. "Democracy in Russia: A Tocquevillian Perspective." In: Aurelian Conversations with Tocqueville. The Global Democratic Revolution in the 21st Century, eds. Aurelian Craiutu and Sheldon Gellar, Rowman & Littlefield. http://prutland.web.wesleyan.edu/Documents/Democracy%20in%20Russia.pdf

Saarinen, Juha. 2010. "Analysis: Who really owns Huawei?" It news, May 28. http://www.itnews.com.au/News/175946,analysis-who-really-owns-huawei.aspx.

Salazar, Javier. 2005. "On the Ontology of MMORPG Beings: A Theoretical Model for Research." In DiGRA 2005 Conference, 1–14.

Sanchez, Julian. 2008. "750,000 lost jobs? The dodgy digits behind the war on piracy." Ars Technica, October 8. http://arstechnica.com/tech-policy/2008/10/dodgy-digits-behind-the-war-on-piracy/

Sandoz, Yves, Zimmermann, Bruno, and Swinarski Christophe. 1987. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Geneva: Martinus Nijhoff Publishers.

Sanger, David E. 2012. "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power." New York: Crown Publishers.

Scaparrotti, Curtis M. 2012. "Joint Publication 3-13 Information Operations". Joint publication. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Schilling, Jeffery. 2010. "Defining our National Cyberspace Boundaries." U.S. Army War College. USAWC Stategy Research Project. Online: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA518322.

Schmitt, Michael N. 2013. Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press.

Schneier, Bruce. 2010. "The Threat of Cyberwar Has Been Grossly Exaggerated." https://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.

Seenan. Gerard. 2004. "Terror groups move into pirated DVDs as profits overtake drugs." The Guardian, July 13. http://www.theguardian.com/uk/2004/jul/13/ukcrime.film

SecureWorks. 2012. "Lifecycle of an Advanced Persistent Threat." http://www.datainfoserver.com/dell_lifecycleofanadvancedpersistentthreat

Shanghai Cooperation Organization. 2001. "The Shanghai Convention on Combating Terrorism, Separatism and Extremism." http://www.sectsco.org/EN123/show.asp?id=68

Shanghai Cooperation Organization. 2006. "Joint Communiqué of Meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation." http://www.sectsco.org/EN123/show.asp?id=95

Shanghai Cooperation Organization. 2007. Bishkek Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation. http://www.sectsco.org/EN123/show.asp?id=92

Sharp, Walter Garry. 1999. "Cyberspace and the Use of Force." Duke Journal of Comparative & International Law. http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1236&context=djcil.

Sharwood, Simon. 2013. "India joins list of nations vetting Huawei, ZTE." The Register, May 10. http://www.theregister.co.uk/2013/05/10/india_to_test_huawei_and_zte_kit/.

Sheehan, Michael. 2011. "The changing character of war." In: The Globalization of World Politics: An introduction to international relation, edited by Baylis, Smith, and Owens, 214–228. Oxford: Oxford University Press.

Sheldon, John B. 2011. "Stuxnet and Cyberpower in War." World Politics Review. Online: http://www.worldpoliticsreview.com/articles/8570/stuxnet-and-cyberpower-in-war.

Sheldon, John B. 2013. "The Rise of Cyberpower." In: Strategy in the Contemporary World: An Introduction to Strategic Studies, edited by Baylis, Wirtz, and Gray, 303–319. Oxford: Oxford University Press, Fourth Edition.

Shimeal, Timothy, Williams, Phil, and Casey Dunlevy. 2001. “Countering Cyber War.” In: NATO Review, Winter 1991-1992, 16-18.

Sidorenko, Alexandre. 2011. “Russia: Digital Oppression Hits Web Forums as Election Approaches.” The Global Voices. http://globalvoicesonline.org/2011/11/22/russia-digital-oppression-hits-web-forums-as-election-approaches/

Singel, Ryan. 2010. “Richard Clarke’s Cyberwar: File Under Fiction.” http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke/.

Siwek, Stephen E. 2007. “The True Cost of Copyright Industry Piracy to the U.S. Economy.” Institute for Policy Innovation, October 2007. http://www.ipi.org/docLib/20120515_CopyrightPiracy.pdf

Skidelsky, Robert. 2012. “After the Crash: The Future of Globalisation.” Survival 54 (3) (November 14): 7–28.

Smith, Eric H., Steven Metalitz, Michael Schlesinger, Eric Schwartz and Amanda Wilson Denton. 2011. “Special 301, Letter to USTR.” International Intellectual Property Alliance, February 15. http://www.iipa.com/rbc/2011/2011SPEC301COVERLETTER.pdf

Smith, Gerry. 2013. “Report For NATO Justifies Killing Of Hackers In A Cyberwar.” The Huffington Post, March 22nd.

Snyder, Jack. 2013. “The Huawei security risk: Factors to consider before buying Chinese IT.“ Search security, January 28. http://searchsecurity.techtarget.com/feature/The-Huawei-security-risk-Factors-to-consider-before-buying-Chinese-IT.

Sovjet pri prezidente. 2013. “Zajavlenja sovjeta.” http://www.president-sovet.ru/council_decision/council_statement/zayavlenie_chlenov_soveta_v_otnoshenii_zakonoproekta_89417_6.php

Souleimanov, Emil, and Karel Svobodal. 2006. “Čečenská válka a ruská společnost.” Central European Political Studies Review 2-3, 8. http://www.cepsr.com/clanek.php?ID=266

Souppouris, Aaron. 2013. “Killing hackers is justified in cyber warfare, says NATO-commissioned report.” The Verge, March 21st.

Stake, Robert E., 1995. "The Art of Case Study Research." London: SAGE.

Stanford Encyclopedia of Philosophy. 2012. “Freedom of Speech”. http://plato.stanford.edu/entries/freedom-speech/

Sterner, Eric. 2011. "Retaliatory Deterrence in Cyberspace." Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011): 62–80. Online: http://www.au.af.mil/au/ssq/spring11.asp.

Sterner, Eric. 2014. "U.S. Failure to Clarify Interests in Cyberspace Weakens Deterrence." World Politics Review, April 11, 2014. Online: http://www.worldpoliticsreview.com/articles/13698/u-s-failure-to-clarify-interests-in-cyberspace-weakens-deterrence.

Stevens, Tim. 2012. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace.” Contemporary Security Policy. Vol. 33:1: 148-170. https://citizenlab.org/cybernorms2012/Stevens2012.pdf

Storm, Darlene. 2012. “Gauss malware: Nation-state cyber-espionage banking Trojan related to Flame, Stuxnet.” http://blogs.computerworld.com/security/20816/gauss-malware-nation-state-cyber-espionage-banking-trojan-related-flame-stuxnet

Sulovic, Vladimir. 2010. “Meaning of Security and Theory of Securitization.” Belgrade Centre for Security Policy, October 5. http://www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf

Sweney, Mark. 2014. “The Walking Dead producer criticises Game of Thrones executive over piracy.” The Guardian, June 19. http://www.theguardian.com/media/2014/jun/19/walking-dead-producer-game-of-thrones-piracy-google

Symantec. 2011. “W32.Duqu: The precursor to next Stuxnet.” http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Symantec. 2012. “Complex Cyber Espionage Malware Discovered: Meet W32.Gauss.” http://www.symantec.com/connect/blogs/complex-cyber-espionage-malware-discovered-meet-w32gauss

Tarakanov, Dmitry. 2013. “The ‘Kimsuky’ Operation: A North Korean APT?” http://securelist.com/analysis/publications/57915/the-kimsuky-operation-a-north-korean-apt/

Tassi, Paul. 2012. “You Will Never Kill Piracy, and Piracy Will Never Kill You.” Forbes, February 3. http://www.forbes.com/sites/insertcoin/2012/02/03/you-will-never-kill-piracy-and-piracy-will-never-kill-you/

Taureck, Rita. 2006. “Securitization theory and securitization studies.” Journal of International Relations and Development, Vol. 9, March 1. http://wrap.warwick.ac.uk/1082/1/WRAP_Floyd_Securitization_theory_and_securitization_studies_WRAP.pdf

Taylor, Josh. 2012. “Huawei reportedly cleared of spying in White House review.“ Zdnet, October 18. http://www.zdnet.com/huawei-reportedly-cleared-of-spying-in-white-house-review-7000005957/.

TERA. 2010. “Building a Digital Economy.” TERA Consultants, The International Chamber of Commerce, March 2010. http://www.iccwbo.org/Data/Documents/Bascap/Economic-Impacts/Tera-study/Building-a-Digital-Economy-TERA

The SecDev Group. 2009. “Tracking GhostNet: Investigating a Cyber Espionage Network.” http://www.f-secure.com/weblog/archives/ghostnet.pdf

Thomas, Timothy L. 2009. "Nation-state Cyber Strategies: Examples from China and Russia." In: Cyberpower and National Security, edited by Kramer, Starr, and Wentz, 465–488. Washington D.C.: National Defense University Press; Potomac Books.

Thornburg, Nathan.2005. “The Invasion of the Chinese Cyberspies.” Time. http://content.time.com/time/magazine/article/0,9171,1098961,00.html

Times of India. 2010. “Desi hackers join Indian cyber army!” http://articles.timesofindia.indiatimes.com/2010-08-05/job-trends/28309456_1_indian-cyber-army-hackers-computer-systems

Townshend, Charles. 2000. The Oxford History of Modern War. New York: Oxford University Press.

Trenin, Dmitri. 2012. "True Partners? How Russia and China See Each Other." London: Centre for the European Reform.

Trenin, Dmitri. 2013. "Russia and the Rise of Asia." Moscow: Carnegie Moscow Center.

Treverton, Gregory F., Carl Matthies, Karla J. Cunningham, Jeremiah Goulka, Greg Ridgeway and Anny Wong. 2009. “Film Piracy, Organized Crime, and Terrorism.” RAND, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG742.pdf

Trustwave. 2014. "Trustwave Global Security Report." http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf?aliId=21867531

Trustwave. 2013. "Trustwave Global Security Report." http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

UK-MoD. 2004. The Joint Service Manual of the Law of Armed Conflict.

United Nations. "Charter of the United Nations." http://www.un.org/en/documents/charter/chapter8.shtml

United Nations Disarmament. 2010. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201).” Study Series 33. http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf

United States Government Accountability Office. 2010. "United States Faces Challenges in Addressing Global Cybersecurity and Governance." Report to Congressional Requesters (GAO-10-606). http://gao.gov/assets/310/308401.pdf

US-CERT. 2005. “Targeted Trojan Email Attacks.” http://www.aub.edu.lb/it/custsupp/alerts/patch/MS/cert/Pages/TA05-189A.aspx

US-DoD. 2011. “Department Of Defense Strategy For Operating In Cyberspace.” http://www.defense.gov/news/d20110714cyber.pdf

Vance, Ashlee and Bruce Einhorn. 2011. “At Huawei, Matt Bross Tries to Ease U.S. Security Fears.“ Businessweek, September 15. http://www.businessweek.com/magazine/at-huawei-matt-bross-tries-to-ease-us-security-fears-09152011.html#p1

Virus Bulletin. 2014. “Command and control.” https://www.virusbtn.com/resources/glossary/command_and_control.xml

Watson, David, Holz, Thornsten, and Sven Mueller. 2005. “Behind the Scenes of Phishing Attacks.” Last modified 16th May 2005. http://www.honeynet.org/papers/phishing/

Web index. 2013. http://thewebindex.org/data/index/

Websense. 2011. “Advanced Persistent Threats and Other Advanced Attacks.” http://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

Webster, Frank. 2006. Theories of the Information Society. Third Edition. London: Routledge.

Wendt, Alexander. 1987. “The Agent-Structure Problem in International Relations Theory.” International Organization 41 (3): 335–370.

Westby, Jody R. (ed.). 2004. International Guide to Cyber Security. Chicago: American Bar Association, Privacy and Computer Crime Committee, Section of Science and Technology Law.

Wilson, Clay. 2008. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” http://www.fas.org/sgp/crs/terror/RL32114.pdf

Witlin, Lauren. 2008. "Of Note: Mirror-Imaging and Its Dangers."SAIS Review of International Affairs, Vol. 28, No. 1 (Winter-Spring 2008): 89–90. Online: http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/sais_review/v028/28.1witlin.html

Xia, Chen. 2013. “Daughter of Huawei founder unveils company's secrets.“ ChinaOrg, January 21. http://www.china.org.cn/business/2013-01/23/content_27774990.htm.

Zimmermann, Andreas. 2007. “The Second Lebanon War: Jus ad bellum, jus in bello and the Issue of Proportionality.” Max Planck Yearbook of United Nations Law, 11: 99-

Ziolkowski, Katharina. 2012. “Ius Ad Bellum in Cyberspace – Some Thoughts on the ‘Schmitt Criteria’ for Use of Force.” In , edited by R. Ottis C. Czosseck. NATO CCD CE Publication

Index

Perspectives on Cybersecurity

Authors: Jakub Drmola, Miroslava Pavlíková, Tomáš Maďar, Lucie Budirská, Petr Suchý, Jakub Harašta, Alena Leciánová, Roman Šulc, Lea Hricikova, Nikola Schmidt

Pre-publishing review: Roman Pačka
Proofreading: Monika Marková

Published by Masaryk University
Brno 2015
1st edition

ISBN 978-80-210-7870-3 (online : pdf)