universität
wien

MASTER THESIS

TITLE

“Wargames in the Fifth Domain”

AUTHOR

Dipl.-Ing.(FH) Karin Kosina

ACADEMIC DEGREE

Master of Advanced International Studies (M.A.I.S.)

Vienna, 2012

Degree Programme code (according to the student record sheet / “Studienblatt”):	A 992 940
Academic discipline (according to the student record sheet / “Studienblatt”):	Postgraduate University Programme International Affairs
Under supervision of:	em. o. Univ.-Prof. Dr. Hanspeter Neuhold

diplomatische
akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

On my honour as a student of the Diplomatic Academy of Vienna, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it.

Vienna, 15 June 2012

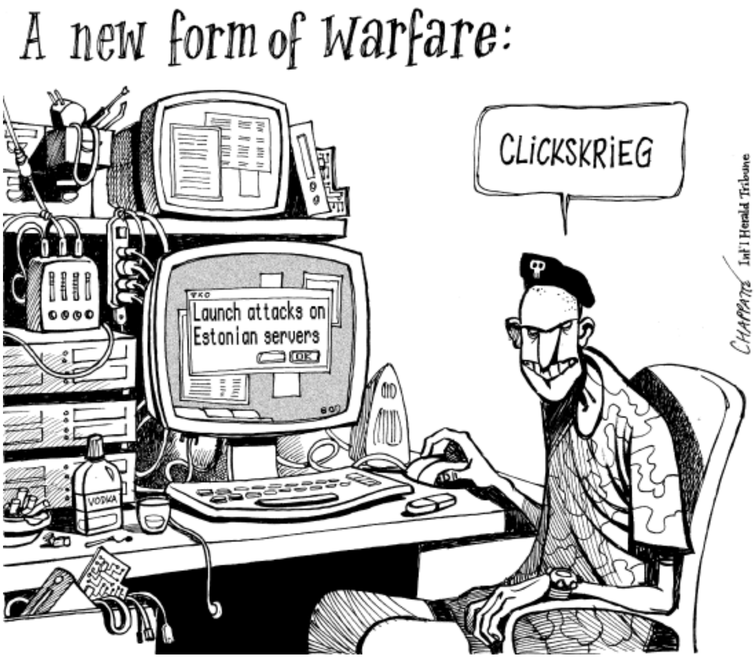

Figure 1: A new form of warfare?

Contents

Chapter 1

Introduction

The next Pearl Harbor could very well be a cyber attack.[1]

This dire warning by Leon Panetta, current US Secretary of Defense and former Director of the Central Intelligence Agency, seems to sum up a grim new reality. Mainstream media coverage merely echoes what top military and intelligence officials appear to agree on: we have entered a "new era of global cyberwar".[2] Malicious hackers are threatening our basic infrastructure, and a "Cyber Katrina"[3] or even a "Cyber 911"[4] appear to be just a matter of time. As Mike McConnell, US Director of National Intelligence from 2007 to 2009, starkly put it:

The United States is fighting a cyber-war today, and we are losing.[5]

Is this really the case though? Is the world indeed facing a new global threat that will surpass terrorism as the greatest danger to the lives and livelihoods of innocent citizens, as FBI Director Robert S. Mueller predicted earlier this year?[6] Or is the cyberwar threat nothing but a "hype fuelling a cybersecurity-industrial complex", a fairytale collection of doomsday scenarios "intentionally hyped up by a coalition of major arms manufacturers, the Pentagon, and Internet security firms greedy for profit" – as detractors of the notion would argue?[7]

This thesis represents an attempt to contribute to the debate on cyber warfare by analysing the actual technical and legal background, separating between known facts and mere speculation. I will aim to show that, as so often, reality is more complex than both high-level officials and the media would have us believe. There *are* serious IT security threats that need to be addressed – threats that could lead to disastrous consequences unless they are adequately dealt with. However, due the nature of these threats – and, in fact, the nature of the global Internet itself – a military response is unlikely to be capable of resolving these issues. On the contrary, by focusing on cyber *warfare*, we risk ignoring the real issues, and even causing a *negative* impact on our digital (and physical) lives.

Motivation

"Cyberwar" has become a hot topic in recent years. Incidents like the cyber attacks against Estonia in May 2007[8], the Stuxnet worm that allegedly sabotaged Iran's nuclear enrichment facility at Natanz in 2009[9], or the recent wave of denial-of-service attacks on Israeli websites, including the Tel Aviv Stock Exchange and national airline El Al[10], have captured the attention of the mainstream media.

Cyberwar is more than just a media catchphrase though. Decision makers on the highest levels have identified it as a major priority. US President Barack Obama has laid out military guidelines for the use of cyber attacks.[11] The Pentagon has established a special command – the *US Cyber Command* – whose mission includes to "conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries".[12] NATO has set up a *Cooperative Cyber Defence Centre of Excellence* in Tallinn, Estonia.[13] NATO Secretary-General Anders Fogh Rasmussen has called cyber attacks "a new form of permanent, low-level warfare".[14] NATO's new Strategic Concept adopted in 2010 lists cyber attacks as a threat that can "reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability"; the strategy determines to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks".[15] The European Union has conducted pan-European cyber attack simulation exercises to "test their responses to a simulated attack from hackers on critical online services"[16] and warned that "attacks against private or government IT systems in EU Member States have given [cyber security] a new dimension, as a potential new economic, political and military weapon".[17] The U.S., Russia, China, North Korea, Israel, Iran, India, and Pakistan have all been accused of engaging in cyber warfare.

However, the current debate on cyberwar is often characterised by a certain lack of depth, technical understanding, and differentiation. The term "cyberwar" itself is ill-defined and tends to be used in a very vague and broad sense. There is indeed a certain hype surrounding the topic that overshadows the underlying information security issues.

Most of the incidents that are usually associated with "cyberwar" are not, in fact, acts of war in the strict sense of the term. Rather, they belong in the domain of (organised) crime, vandalism, espionage, or "hacktivism". Using the framework of *war* for dealing with these activities is both counterproductive and dangerous. The problem with overusing the cyberwar metaphor is two-fold:

On the one hand, the militarisation of the debate leads to dangerous fallacies in how to best approach the defence against cyber attacks. Suggestions such as the *Internet Kill Switch* bill proposed by US Senator Joe Lieberman in 2010 are the result of trying to apply military thinking to the civilian virtual domain.[18] Lieberman's bill would have given the President the authority to disconnect the US from the Internet in case of an emergency. This is a deeply problematic idea. It is based on fundamentally flawed assumptions, including the notion that cyberspace has traditional borders that can be protected by a kind of "electronic Maginot Line".[19] This is not the case. It simply would not work to isolate a specific territorial part of the Internet, and – given the dependence of public and private infrastructure on the global network – trying to do so would create any number of unpredictable side effects.

On the other hand, a primarily military approach is ill-suited to actually decreasing the possibility of cyber attacks and improving the security of critical infrastructure. To do this, a comprehensive approach to increasing general IT security levels and infrastructural resilience is needed, with the main actors being the public and business sectors. Increased awareness, transparency, cooperation, and risk management are the key terms - neither of which can be implemented by military doctrine.

My main motivation in writing this thesis is to encourage a more differentiated understanding of the threats imposed by today's increasingly interconnected and digitalised infrastructure. I call for a reversal of the trend to militarise our approach to these threats, and for a reframing of the debate in *civilian* terms.

Methodology

As all M.A.I.S. theses, this is an interdisciplinary work. The main academic disciplines of this thesis are political science and international law. Due to the nature of the topic I also touch upon many issues that belong into the domains of computer science in general and information security in particular. My approach is to combine a literature study from the relevant fields with a practical perspective from experts and professionals, based on statements published in the media as well as personal interviews. This includes input from researchers and practitioners from the information security community and the intelligence community, as well as members of the "hacker scene".

A note on the technical issues discussed in this work: None of the technical material I present is new. In fact, all the threats I discuss are well-understood at this point, and volumes of in-depth analysis have been published on them. However, these technical reports are written for a very specific audience – namely the information security community – and as such they tend to be somewhat opaque to readers from other disciplines. Or, as one of the information security experts I discussed this with put it, “No wonder normal people have difficulties understanding IT security. It’s almost as if we are proud of writing in geek speak rather than plain English.” This may be one of the reasons why the discussion of “things cyber” among the general public tends to be rather one-dimensional, echoing the stories from the above-mentioned newspaper headlines. One of my goals in writing this thesis is to translate the main points from the relevant information security literature from “geek speak” into English. I hope that this will contribute to a more comprehensive and differentiated discussion of what is really going on, and make it easier to separate between known facts and the tentative conclusions that might be drawn from these facts.

Structure

This thesis is structured as follows: Chapter 2 attempts to establish a definition of cyberwar. Chapter 3 explains the most common cyber attacks and presents the different actors that may use cyber attacks and their motivations. The legal dimension of cyber warfare is discussed in Chapter 4. Chapter 5 presents a number of cyber incidents and analyses whether each of them would qualify as an act of (cyber) war. A detailed case study of the *Stuxnet* incident in Chapter 6 shows the potential and limitations of cyber warfare in practice. Chapter 7 presents my argument why, despite all claims to the contrary, cyberwar is probably not imminent – and why a different approach is needed to deal with the real cyber threats we are facing today. Based on this analysis, Chapter 8 makes some recommendations for concrete steps to be taken to address these threats. Finally, Chapter 9 concludes the thesis.

Cyberwar is a complex topic. As General Michael V. Hayden, former Director of the NSA and of the CIA, remarked,

> *Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon.*[20]

Obviously, a work as limited in scope as this one can merely scratch the surface of the issues we are dealing with. Even so, it is my hope that this thesis will succeed in adding some clarity and understanding to this crucial debate.

Notes

[1] "CIA chief Leon Panetta: The next Pearl Harbor could be a cyberattack", *The Christian Science Monitor*, 9 June 2011, http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

(Note: Unless explicitly mentioned otherwise, all hyperlinks were last accessed on 14 June 2012.)

[2] Peter Beaumont, "Stuxnet worm heralds new era of global cyberwar", *The Guardian*, 30 September 2010, http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

[3] David Kravet, "Vowing to prevent 'Cyber Katrina,' Senators propose Cyber Czar", *Wired*, 1 April 2009, http://www.wired.com/threatlevel/2009/04/vowing-to-preve/

[4] Tabassum Zakaria, "Former CIA official sees terrorism-cyber parallels", *Reuters*, 3 August 2011, http://www.reuters.com/article/2011/08/03/us-usa-security-cyber-idUSTRE7727AJ20110803

[5] "Mike McConnell on how to win the cyber-war we're losing", *The Washington Post*, 28 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[6] Robert S. Mueller, III, "Combating threats in the cyber world: Outsmarting terrorists, hackers, and spies". Speech at the RSA Cyber Security Conference, San Francisco, CA, 1 March 2012, http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[7] "Is cyberwar hype fuelling a cybersecurity-industrial complex?", *RT TV*, 17 February 2012, http://rt.com/usa/news/security-us-cyber-threat-529/

[8] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

[9] See Chapter 6 for a detailed discussion of the Stuxnet incident.

[10] Isabel Kershner, "2 Israeli web sites crippled as cyberwar escalates", *The New York Times*, 16 January 2012, http://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html

[11] "Obama hands military new cyber war guidelines", *CBS News*, June 22, 2011, http://www.cbsnews.com/stories/2011/06/22/scitech/main20073212.shtml

[12] U.S. Cyber Command, http://www.arcyber.army.mil/

[13] CCDCOE, http://www.ccdcoe.org/

[14] Siobhan Gorman, "Cyber attacks test Pentagon, allies and foes", *The Wall Street Journal*, 25 September 2010, http://online.wsj.com/article/SB10001424052748703793804575511961264943300.html

[15] NATO, "Active Engagement, Modern Defence. Strategic concept for the defence and security of the Members of the North Atlantic Treaty Organisation", 19 November 2010, http://www.nato.int/

lisbon2010/strategic-concept-2010-eng.pdf

[16] "Digital Agenda: cyber-security experts test defences in first pan-European simulation", EU press release IP/10/1459, 4 November 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1459

[17] "Report on the Implementation of the European Security Strategy – Providing Security in a Changing World", S407/08, 11 December 2008, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

[18] Declan McCullagh, "Bill would give president emergency control of Internet", *CNET News*, 28 August 2009, http://news.cnet.com/8301-13578_3-10320096-38.html.

For an analysis of the legal aspects of the proposal, see Paul Rosenzweig, "The Internet 'Kill Switch' Debate", *Lawfare*, 2 February 2012, http://www.lawfareblog.com/2012/02/the-internet-kill-switch-debate/

[19] Bruce Schneier, "3 reasons to kill the Internet Kill Switch idea", *Schneier on Security*, 9 July 2010, http://www.schneier.com/essay-321.html

[20] Michael V. Hayden, *The Future of Things Cyber* (Hayden 2011, p. 3).

Chapter 2

What is Cyberwar?

2.1 Definition

"Cyberwar is coming!", John Arquilla and David Ronfeldt predicted already in 1993.[21] In 1995, speaking to the Armed Forces Communications-Electronics Association, Air Force chief of staff Gen. Ronald R. Fogleman pointed out that warfare is about to expand into a new domain:

> If you use as your starting point the beginning of the 20th century, you recognize that war has been fought in two dimensions – on land and at sea. [...] Then, with the airplane, warfare took on a third, vertical dimension. [...] I think the next major advance came in the Space Age. This is the fourth dimension of warfare. [...] *I think it is appropriate to call information operations the fifth dimension of warfare.* Dominating this information spectrum is going to be critical to military success in the future.[22]

In 2010, William J. Lynn III, then U.S. Deputy Secretary of Defense, confirmed that this prediction had become reality:

> As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it.[23]

However, almost twenty years after Arquilla and Ronfeldt's proclamation of the advent of cyberwar, there is still no consensus on what *cyberwar* actually means. Experts on national security not only disagree on the definition – they appear to hold diametrically opposed opinions on whether such as thing as cyberwar even exists. As mentioned in the introduction, Mike McConnell, former U.S. Director of National Intelligence, is convinced that the United States are not only fighting a cyberwar today but that they are in the process of losing it.[24] Howard Schmidt, the current cyber-security coordinator (aka "cyber czar") at the White House, does not think so. On the contrary, in an interview just one week after McConnell's dire warning, Schmidt stated:

> There is no cyberwar. I think that is a terrible metaphor and I think that is a terrible concept.[25]

Setting aside for the moment the question of whether it makes sense to speak of an ongoing cyberwar – this is one of the questions that the remainder of this thesis is trying to answer –, let us consider what such a cyberwar would look like.

Richard A. Clarke, former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism and co-author of the best-selling book *Cyber War: The Next Threat to National Security and What to Do About It*, defines cyberwarfare as

> actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.[26]

This definition is fairly loose though and would include many incidents that should not be properly considered acts of war. (I will get back to the issue of what constitutes an armed attack in cyberspace in Chapter 4.) A better definition is suggested by Peter Sommer and Ian Brown in a comprehensive report written for the OECD *Future Global Shocks* project in 2011:

> A true cyberwar is an event with the characteristics of conventional war but fought exclusively in cyberspace.[27]

Two aspects of this definition deserve our attention: Sommer and Brown point out that one, a cyberwar would have to cause real-world damage comparable to that of a regular (non-cyber) war, and two, a proper cyberwar would be fought in cyberspace only.

The first idea is a central one. All too often, the discussion around cyberwar treats all cyber attacks as equivalent. Minor incidents that are the online equivalent of vandalism or petty crime are thus elevated to the level of armed attack. However, the same standards that are used for traditional warfare should also apply in the digital domain.

As James Lewis, senior fellow and Director of Technology and Public Policy at the Center for Strategic and International Studies in Washington, D.C., clarifies:

> Cyberwar has to meet the same threshold we'd hold any other war to. So if someone spray-painted a government building with graffiti, we wouldn't call that an attack. And if someone is caught spying, that isn't war. There has to be physical destruction, and there have to be casualties. If there aren't, it isn't an attack, and it isn't war.[28]

This notion is known as *cyber equivalence*. A cyber attack should only be considered use of force (and thus an act of war that may merit military retaliation) if it results in an amount of death, damage, destruction or high-level disruption comparable to that which a traditional military attack would cause.[29]

The second aspect of cyberwar being "fought exclusively in cyberspace" is interesting as well. There is no doubt that nation states will make use of information technology for purposes of warfare. Cyber attacks can be used in combination with conventional "kinetic" weapons and play an important role as force multipliers. This does not make future wars into cyberwars though, just as the use of airplanes in the First World War did not make that war an "airwar".

Thomas Rid uses a similar approach to analysing whether or not a cyber attack actually constitutes an act of war. By his definition, cyberwar is

> a potentially lethal, instrumental, and political act of force conducted through malicious code.[30]

I will refer to Rid's framework in my subsequent discussion of cyber incidents as potential acts of cyberwar, so I will present it in somewhat more detail here. Rid bases his definition of cyberwar on the traditional understanding of war as laid out by Carl von Clausewitz. According to Clausewitz, the concept of war has three main elements. The first element is that war is violent. As Rid explains: "If an act is not potentially violent, it is not an act of war. Then the term is diluted and degenerates to a mere metaphor, as in the 'war' on obesity or the 'war' on cancer. A real act of war is always potentially or actually lethal, at least for some participants on at least one side."[31] The second element is that an act of war is always instrumental, in the sense that it is a mere means to achieve an end – forcing the enemy to accept the offender's will. The third element is the political nature of war. An act of war is part of a larger political purpose, as expressed by Clausewitz's famous phrase, "War is a mere continuation of politics by other means".[32]

In conventional armed confrontation it is usually straightforward to identify acts of force. The result of a bombing raid or a drone strike is direct and immediate. In cyberspace, the situation is more complex, since the sequence of events that lead to actual violence is generally indirect: "The causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction. Yet such mediated destruction caused by a cyber offense could, without doubt, be an act of war, even if the means were not violent, only the consequences."[33]

Actions carried out in cyberspace could thus be acts of war. However, as the subsequent chapters of this thesis will show, most of the cyber attacks that have been observed so far clearly do *not* qualify.

Determining whether a cyber act may be an act of (cyber) war is more difficult than it may seem at first. Even when it is clear that a cyber attack meets the criteria of "equivalent" violence (and again, most attacks we have seen do not), it has to be established that a state actor was responsible for the attack. For technical reasons, it is rarely possible to do so conclusively. This is known as the problem of *attribution*, and is discussed in detail in Chapter 3.

2.2 Cyberwar in Military Strategy

It is instructive to also consider the practical definition of cyberwar as reflected in military strategy. As an example, I will discuss the understanding of cyber operations as put forth by the U.S. Department of Defense. Obviously, the U.S. is not the only state that has identified cyberspace as an important operational domain. However, unlike other states known or suspected of developing active and passive cyber warfare capabilities, the U.S. Department of Defense releases unclassified public versions of strategic documents, which makes it easier to evaluate their position.

The U.S. Department of Defense has formally recognised cyberspace as a new domain of warfare. The Pentagon's *Strategy for Operating in Cyberspace*, released in July 2011, states that "DoD will treat cyberspace as an operational domain".[34] The term "cyberspace" here refers to the definition first set out by the Joint Chiefs of Staff in the U.S. *National Military Strategy for Cyberspace*:

> Cyberspace is a domain characterized by the use of electronics and the

> electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.[35]

The U.S. Department of Defense's *Strategic Guidance* document, released in January 2012, lists as one of the primary missions the ability to "operate effectively in cyberspace". This includes building the capacity for U.S. forces to conduct "a combined arms campaign across all domains – land, air, maritime, space, and cyberspace" and to "invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace".[36]

Neither the 2011 Strategy for Operating in Cyberspace nor the 2012 Strategic Guidance define what would be considered an act of cyberwar or what the response to such an act would be.

The lack of clarity in the Pentagon's cyber strategy was criticised by Senator John McCain during a Senate Armed Services Committee hearing on 19 July 2011. Senator McCain pointed out that "fundamental questions" were unanswered, specifically what moves in cyberspace would be considered "hostile actions" and when and how the military would react.[37] To my knowledge, these questions have not been adequately addressed so far.

Some light on the U.S.' understanding of cyber attacks and how they would respond to them was shed by a November 2011 report to Congress by the Department of Defense. *Senate Report 111-201*, accompanying the National Defense Authorization Act For Fiscal Year 2011, had posed thirteen specific questions on cyber policy to the Department of Defense and the U.S. Government.[38] The answers to these questions made it clear that a response to a cyber attack need not be limited to a counter-attack in cyberspace, but may be escalated to include kinetic means, i.e. conventional weapons:

> The President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber *and/or kinetic capabilities* provided by DoD.[39]

Nowhere does the report specify what constitutes a "significant cyber attack" – in my opinion a prime example of constructive ambiguity that intentionally leaves room for future interpretation. Ultimately, no-one seems to really know what cyberwar will look like, if and when it does happen.

Notes

[21] John Arquilla and David Ronfeldt, *Looking Ahead: Preparing for Information Age Conflict* (Arquilla and Ronfeldt 1997, p. 23).

[22] Ronald R. Fogleman, “Information Operations: The Fifth Dimension of Warfare”, Remarks as delivered to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995, `http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm`. (Emphasis added.)

[23] William J. Lynn III, *Defending a New Domain. The Pentagon’s Cyberstrategy* (Lynn III 2010). Article also available online at the U.S. Department of Defense website, `http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx`

Incidentally, the term *cyberspace* was coined by Science Fiction author William Gibson. In Gibson’s own words, “Somehow I knew that the notional space behind all of the computer screens would be one single universe. [I had to] name it something cool, because it was never going to work unless it had a really good name. So the first thing I did was sit down with a yellow pad and a Sharpie and start scribbling – infospace, dataspace. I think I got cyberspace on the third try, and I thought, Oh, that’s a really weird word. I liked the way it felt in the mouth–I thought it sounded like it meant something while still being essentially hollow.” See David Wallace-Wells, “William Gibson, The Art of Fiction No. 211”, *The Paris Review*, Summer 2011, `http://www.theparisreview.org/interviews/6089/the-art-of-fiction-no-211-william-gibson`

[24] “Mike McConnell on how to win the cyber-war we’re losing.”, *The Washington Post*, 28 February 2010, `http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html`

[25] Howard Schmidt, quoted in Ryan Singel, “White House Cyber Czar: ’There Is No Cyberwar”’, *Wired*, 4 March 2010, `http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/`

[26] Richard A. Clarke, *Cyber War. The Next Threat to National Security and What to Do About It* (Clarke 2010, p. 6).

[27] Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risk* (Sommer and Brown 2011, p. 6).

[28] Stuart Fox, “Cyberwar: Definition, Hype & Reality”, *Security News Daily*, 2 July 2011, `http://www.securitynewsdaily.com/828-cyberwar-definition-cyber-war.html`

[29] Siobhan Gorman, “Cyber Combat: Act of War”, *Wall Street Journal*, 30 May 2011, `http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html`

[30] Thomas Rid, *Cyber War Will Not Take Place* (Rid 2012, p. 5).

[31] (Rid 2012, p. 7)

[32] *‘’Der Krieg ist einer bloße Fortsetzung der Politik mit anderen Mitteln”* – Carl von Clausewitz, *Vom Kriege* (von Clausewitz 1832, p.44).

[33] (Rid 2012, p. 9)

[34] U.S. Department of Defense, “Department of Defense Strategy for Operating in Cyberspace”, July 2011, `http://www.defense.gov/home/features/2011/0411_cyberstrategy/`

docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf

[35] Chairman of the Joint Chiefs of Staff, “National Military Strategy for Cyberspace Operations”, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

[36] U.S. Department of Defense, “Sustaining U.S. Global Leadership: Priorities for 21st Century Defense”, strategic guidance document, January 2012, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

[37] John T. Bennett, “Senators: US needs to define acts of cyberwar”, *The Hill*, 19 July 2011, http://thehill.com/blogs/hillicon-valley/technology/172247-us-needs-to-define-an-act-of-cyberwar-senators-say

[38] Senate Report 111-201, *Library of Congress*, 4 June 2010, http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp1111Nlmz&r_n=sr201.111&dbname=cp111&&sel=TOC_215632&

[39] U.S. Department of Defense, “Cyberspace Policy Report”, report to Congress pursuant to the National Defense Authorization Act for fiscal year 2011, section 934, November 2011, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (Emphasis added.)

Chapter 3

The Threat Landscape

One of the main problems in the contemporary discourse on cyberwar is that cyber attacks are often treated in an indiscriminate way. However, the spectrum of aggressive incidents perpetrated online is large, encompassing different technical means, levels of sophistication, amounts of damage, attackers, and motives. As information security expert Rafal Rohozinski points out:

> We need to arrive at a more graded definition of cyber attacks. Now we have this universal way of talking about them, which doesn't allow for different definitions of culpability.[40]

Any "bad act" committed online does not automatically equate an act of cyberwar. That does not mean that such acts are not to be taken seriously – quite the contrary. But conflating the threats does nothing to improve cyber security, and actually makes it harder to deal with them constructively and appropriately. Theft, vandalism, and industrial espionage are all serious problems. No-one would consider them acts of war though. The same is true online. Theft, vandalism, and industrial espionage committed via the Internet are still theft, vandalism, and industrial espionage. They are to be taken seriously, but they are appropriately dealt with using the civilian legal system – not by crying war and calling in the troops.

Therefore, this chapter presents an overview of the different kinds of attacks and the different kinds of attackers, explaining the differences in their technical sophistication, motivation and results.

3.1 Cyber Attacks

3.1.1 Denial of Service (DoS)

A denial-of-service (DoS) attack is an attempt to make an online resource – often a website – unavailable to its legitimate users. DoS attacks work by "flooding" the resource with a large number of requests. This overwhelms the server, which is no longer capable of responding to all the requests. Regular users trying to use the resource are thus not able to get access.

A DoS attack originating from one source computer would be easy to block. Therefore most DoS attacks are *distributed* denial-of-service (DDoS) attacks. This simply means that the attack originates from more than one source, i.e. a large number of computers sending requests to the same server.

DDoS attacks can be conducted by having computer users voluntarily join forces to participate in the attack. More commonly, DDoS attacks are orchestrated using *botnets* – networks of compromised computers whose users are not even aware that their machines are involved in an attack.[41] Malicious software (*malware*) installed on the computer allows a third-party – the actual attacker – to take control of the machine and turn it into a *bot* (short for robot) participating in the DDoS attack. Botnets are usually set up and operated by organised criminal groups who rent them out to aspiring DDoS attackers – at what may seem like surprisingly low rates. A study conducted in 2010 found that hourly botnet rental pricing started at $8.94, with the average price for renting a botnet for twenty-four hours being $67.20.[42]

Denial-of-Service attacks are among the most wide-spread cyber attacks. The oft-cited "cyberwar" on Estonia in April 2007 (see Chapter 5, p. 43 *ff.* for details) consisted of a series of DDoS attacks.

It is important to understand that DDoS attacks are at the lowest end of the spectrum when it comes to cyber attacks. They cause no lasting damage, are comparatively easy to protect against, and are trivial to orchestrate if one has either enough money to rent a botnet or enough supporters who are willing to contribute their resources to the attack. As Jose Nazario of Arbor Networks pointed out, a DDoS attack requires "just a lot of people getting together and running the same tools on their home computers".[43] Even more importantly, a DDoS attack just means that the attacked resource, for instance a website, is temporarily unavailable. A DDoS attack alone does *not* mean that the attackers got access to any of the data on the targeted machine or were able to do any other harm.

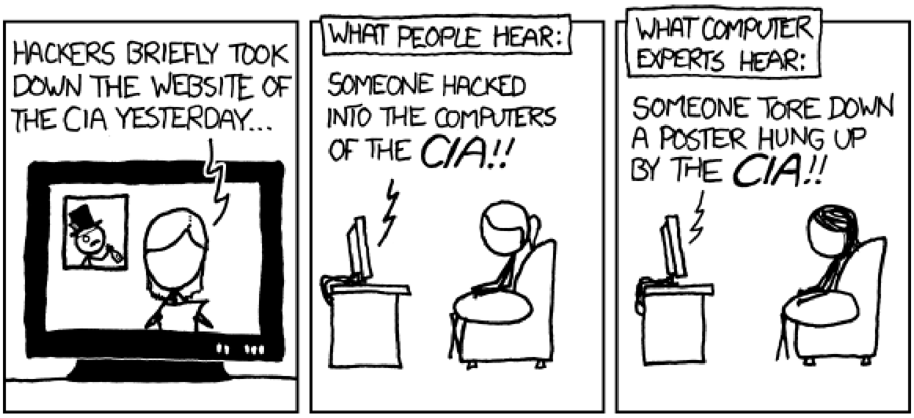
HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

Figure 2: Hackers took down the website of the CIA.

The basic technical distinction between a DDoS attack and actually gaining access to a system is often (intentionally or unintentionally) misrepresented in the media. A mere DDoS attack is portrayed as *Evil Enemy X* having "hacked into" *Critical or Sexy-Sounding Target Y*. This conflation is so common that is has given rise to a standing joke in the information security community, depicted in Figure 2 above.

For instance, on 15 June 2011, members of the hacker group *LulzSec* committed a DDoS attack against the website of the Central Intelligence Agency, succeeding in briefly making the site inaccessible. According to media reports, this was an impressive (and scary) achievement: "In what's sure to be among the most brazen cyber-attacks in history, the hacker group LulzSec took down the website of the Central Intelligence Agency Wednesday evening (June 15)".[44]

In reality, though, this does not mean much. Websites are generally run on separate infrastructure that is not connected to more critical, internal networks. Usually, the web server is not even at the same location as the actual organisation but hosted by an outside web hosting company. Like any DDoS attack, the attack against `http://www.cia.gov` did not mean that *LulzSec* had gotten access to the CIA's web server – let alone the CIA's internal network. It just meant that they had, for a very short period until the web hosting company responded to the attack, made it impossible for people to look at the website. Not so impressive in the end.

According to the definition outlined in Chapter 2, a DDoS attack is clearly not an act of cyberwar, since the component of violence is missing. There is no lasting damage. DDoS attacks only cause inconvenience (to Internet users who are temporarily unable to access the targeted resource), and financial loss (through the IT specialists and extra technical resources needed to deal with the attack). As security expert Bruce Schneier explains, only half in jest:

> A real-world comparison might be if an army invaded a country, then all got in line in front of people at the DMV so they couldn't renew their licenses. If that's what war looks like in the 21st century, we have little to fear.[45]

3.1.2 Website Defacement

A *website defacement* is an attack on a website that changes the content of that website. Often the new content reflects the motivation of the attacker (for instance stating his or her political or ideological believes), ridicules the target, or both.

One of the most common methods for website defacements is a technique known as *SQL injection*. In an SQL injection attack, the attacker is able to pass commands to a database by entering malicious data in a web form.[46] In theory, SQL injections are easy to protect against, since they are only possible due to programming errors in the website. However, in practice many websites are vulnerable to them due to lax security practices.

Contrary to DDoS attacks, a website defacement means that the attacker actually succeeded in getting access to the target computer. However, as explained above, being able to get into an organisation's web server is not the same as breaking into that organisation's internal network, since web servers are usually hosted on a different network.

A well-known website defacement happened during the cyber attacks on Georgian websites in August 2008, when unknown attackers gained access to the website of the Parliament of Georgia and posted a collage of pictures of Adolf Hitler and Georgian President Mikhail Saakashvili. (See Chapter 5, p. 45 *ff.* for more on the Georgian "cyberwar".)

Website defacements do not constitute acts of war since their only result is some embarrassment (to the website owner) and potentially financial loss (due to the legitimate content of the website being inaccessible and/or damage to the owner's public image).

3.1.3 Other Break-Ins

A more serious issue are break-ins into computers other than mere web servers (or break-ins into web servers if these machines are used to store data other than just the public website). Such break-ins can be perpetrated using techniques similar to the ones used for website defacement, such as SQL injection.

The difficulty of a break-in depends on the IT security level of the target system. Once an attacker has gained access to a machine, they may be able to access other computers on the same network, steal confidential data, install malware to turn machines into zombies for a botnet (see above), or cause other damage.

It is impossible to make generalised statements about computer break-ins, except to say that a break-in itself does not constitute an act of war. However, the *results* of the break-in might – in the very unlikely case that the attacker was able to, say, cause significant physical damage by manipulating an Industrial Control System.

3.1.4 SCADA Attacks

SCADA is a technical term that stands for *Supervisory Control and Data Acquisition*. The purpose of SCADA systems is to control and monitor industrial processes. For instance, they can be used to operate assembly lines – but also to control critical functions at power plants.

SCADA systems have been around for decades, but they used to be isolated. Nowadays more and more SCADA systems are connected to the Internet or accessible using devices like USB sticks. This means more convenience and flexibility for the operators, but it also makes these systems susceptible to cyber attacks.[47]

In 2011, IT security researcher Éireann P. Leverett discovered that more than 10,000 such industrial control systems were connected to the Internet, including water and sewage plants. Many of these systems were easy targets for an attack due to lax security practices. For instance, only 17 percent of the systems required authorisation to connect. This indicates that either the operators had failed to take the most basic security precautions – or that they were simply not aware that their systems were online at all.[48] When Leverett's work was presented at the S4 IT security conference, an employee of Schweitzer, one of the major industrial control systems companies, confirmed this. He said that after notifying customers whose systems were found online, at least one of them responded, "We didn't even know it was attached".[49]

If an attacker can get access to a SCADA system, he or she may be able to perform all the functions that the legitimate operator of the system would have access to. Needless to say, this is a very dangerous threat. Unfortunately, the current security standards for SCADA systems appear to be seriously lacking. Improving the security of industrial control systems should be one of the main priorities when dealing with cyber threats. As Thomas Rid put it:

> We don't see enough pressure on control systems vendors and creators, security in these areas is often shocking and I don't know how they've got away with it for so long.[50]

However, despite all the horror scenarios presented in the media, so far there is only one known incident where an attacker gained access to an industrial control system – the *Stuxnet* worm, described in detail in Chapter 6.

SCADA attacks have the potential to result in real-world damage that may reach a level comparable to a conventional armed attack, so they might qualify as acts of war. However, the problem of attribution would be a crucial issue (see below).

3.2 Cyber Attackers

Given the success of the Internet as a platform for commerce, collaboration, and social exchange, it comes as no surprise that while enabling countless positive human activities, the whole spectrum of negative activities is reflected in cyberspace as well. Among the threats encountered in cyberspace, cybercrime is by far the largest. Cyber espionage – both state- and corporate-sponsored – is another threat. There are also hackers following other, more complex motives, such as "hacktivists" or individuals attacking computer system just because they can – *for the lulz*, as the saying in the hacker community goes.

When analysing whether a cyber attack may be an act of cyberwar, the question of the attacker's identity (and, to a lesser degree, their motive) is essential. A useful framework for analysing cyber attacks in this regard has been suggested by Thomas Rid: He points out that regardless of whether computers are involved or not, aggression spans a spectrum ranging from purely criminal acts to purely political acts, with the majority of offences lying in the area between the two extremes. On the one end of the spectrum there is conventional war, which is always political; on the other end is ordinary crime, which is mostly apolitical. Activities between these two poles constitute "political violence" or "political crime", which may involve states as well as private actors. Political crime includes subversion, espionage, and sabotage. Rid points out that the majority of cyber attacks are criminal acts, while none of them are acts of war.

Some attacks constitute what he terms “political cyber offenses” – online variants of subversion, espionage, or sabotage:

> All known political cyber offenses, criminal or not, are neither common crime nor common war. Their purpose is subverting, spying, or sabotaging. [...] It goes without saying that subversion, espionage and sabotage – “cybered” or not – may accompany military operations. Both sides may use it, and indeed have done so since time immemorial.[51]

A special case not directly covered by Rid’s framework is terrorism – non-state actors pursuing political goals by violent means. It would be beyond the scope of this work to go into the complexities surrounding the phenomenon of terrorism. Suffice it to say that, the controversies following the September 11 attacks notwithstanding, terrorist incidents are generally regarded as criminal acts rather than acts of war, which would also be true for hypothetical acts of cyber terrorism.[52]

3.2.1 Cybercrime

Cybercrime is big business. In 2011, the global cybercrime market was more than $12.5 billion. Taking the Russian segment of cybercrime as an example: The Russian national cybercrime market was $2.3 billion in 2011, almost doubling in size from the previous year’s number of $1.2 billion. The most profitable kinds of criminal activities were online fraud (totalling $942 million), spam ($830 million), cybercrime to cybercrime (C2C) – yes, this actually exists – including “services for anonymization and sale of traffic, exploits, malware, and loaders” ($230 million) and DDoS ($130 million).[53]

According to Costin Raiu, anti-virus expert at the Russian security company Kaspersky Lab, there are three factors that make cybercrime so attractive for criminals: First, cybercrime is highly profitable. Second, cybercrime is low-risk. And third, and most importantly, cybercrime is mostly anonymous due to the difficulty of attribution.[54]

Cybercrime is certainly the single largest cyber threat. It is clear, however, that criminal actions *per se* – including actions perpetrated by transnational organised criminal groups – are not acts of war. Cybercrime is an important issue to deal with, but it falls clearly into the domain of civilian law enforcement.

3.2.2 Hacktivism

Hacktivism is a neologism of unknown origin blending the words *hacking* and *activism*. Hacktivists are individuals who engage in hacking activities, including trying to gain unauthorised access to a computer or network, in order to further social or political ends.

An example of a hacktivist group is *Anonymous*, a loose and leaderless collection of activists who unite around a self-defined cause. Anonymous' motto is *We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.* Some of the activities undertaken by the Anonymous collective are clearly political in nature; others are more properly seen as a form of entertainment – *doing it for the lulz*, merely for the "fun" of it.[55]

Hacktivism is not a genuinely new concept. Essentially, it is simply the online expression of other activities associated with activism, which may (but usually do not) include criminal offences. As Peter Sommer, a visiting professor at the London School of Economics, explains: "There is nothing new in what the hacktivists are doing. It really should not be exaggerated. It's really more like the kind of thing Greenpeace does."[56] Sommer further clarifies this point in an OECD report on reducing systemic cybersecurity risk that he co-authored: "A short-term attack by hacktivists is not cyberwar [...] but is best understood as a form of public protest."[57]

In the framework of Thomas Rid outlined above, hacktivism falls into the grey area between politics and crime, most closely resembling what is traditionally understood as subversion – "the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order."[58] Subversion is not an act of war, and neither is hacktivism.

3.2.3 Cyber Espionage

Espionage can be defined as "an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information".[59]

Espionage can be primarily social or primarily technical in nature, a distinction referred to as HUMINT (human intelligence) vs. SIGINT (signals intelligence) in Western intelligence communities. Needless to say, the Internet provides an excellent SIGINT platform and is widely used for purposes of cyber espionage.

Corporate espionage falls into the realm of economic crime and thus clearly does not constitute an act of (cyber) war. As for espionage conducted by state actors: The great majority of state-sponsored (or to put it more accurately, assumedly state-sponsored) cyber attacks have been cases of espionage. I am not going to go into the legal or moral merits of espionage here; suffice it to say that espionage is generally not considered an act of war, so the same should apply to espionage conducted online. As international law professor Charles J. Dunlap Jr. points out, "nondestructive computer methodologies employed for espionage may violate the domestic law of the victim nation-state but are not contrary to international law".[60] Cyber espionage should thus not be treated differently from espionage in general:

> Some people say cyberespionage is just a few clicks away from cyberwar. It's not; it's just another way of spying.[61]

3.2.4 Others

The motivations portrayed above account for the majority of cyber incidents. However, state or non-state actors may also use the Internet for other purposes.

One potential attack scenario would be for state actors to commit sabotage via a cyber attack. An act of sabotage is a "deliberate attempt to weaken or destroy an economic or military system.".[62] Sabotage does not automatically constitute an act of war since the saboteurs may deliberately avoid (open) violence and political attribution. However, an act of cyber sabotage might be considered an armed attack *if* – and that is a crucial *if* – attribution to a state actor could be established. The Stuxnet attack (discussed in detail in Chapter 6, p. 57 *ff.*) may have been an act of cyber sabotage.

In theory, terrorists could also use cyber attacks to perpetrate acts of violence – a threat that has seen much media hype in recent years. However, so far there has not been a single reported incident of cyber terrorism. Moreover, there is no publicly available information indicating that any terrorist group currently has the capability to launch serious cyber attacks. As an analysis by information security researcher Irving Lachow concluded,

> It is difficult to assess with certainty the risks posed by cyber terrorism. However, there is strong circumstantial evidence pointing to the conclusion that terrorist groups are limited to launching simple cyber attacks and exploiting existing vulnerabilities. [...] It appears that terrorist groups in general do not have the expertise to conduct advanced or complex cyber attacks.[63]

Lachow suggests that this is both due to the high level of knowledge and skills that a cyber terrorist attack would require, and to the fact that physical attacks are more attractive to terrorists:

> In comparison to cyber terrorism, using physical means to create terror is fairly easy to do and is quite effective. From a terrorist perspective, cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events. While it is possible that a complex attack on a critical infrastructure would create some of these desired effects, including a sense of panic or a loss of public confidence, terrorists appear incapable of launching such attacks in the near future. Faced with a choice between conducting cyber attacks that would be viewed mostly as a nuisance or using physical violence to create dramatic and traumatic events, terrorists have been choosing the latter.[64]

3.3 The Attribution Problem

A key feature of cyber attacks is that it is very difficult, usually impossible, to establish the identity of the perpetrator.[65] This is not because cybercriminals and other attackers are particularly clever. Rather, it is due to the basic design of the Internet. Cyber attackers can employ a variety of technical means to hide their identity. They also tend to make use of unwitting third parties' computers for their nefarious activities. In order to understand how this works, let us consider some of the basic building blocks of the Internet:

Generally, each machine on the Internet has a unique IP address – a string of numbers that identifies the machine and its location. For instance, the IP address of the machine I am writing this on is 178.209.51.173.[66] This number is unique, and points not only to my logical address on the Internet but also to my current physical location, an apartment in the outskirts of Bratislava. If you saw an attack coming from 178.209.51.173, you would know that it comes from this specific computer. By involving the competent law enforcement authorities, you could then determine the identity of the apparent attacker – the person to whom that IP address was assigned at the time: me.

However, an actual attacker would be aware of this, and take steps to hide the origin of the attack. One way to do this is to use *IP spoofing*, a technique by which an attacker changes his or her address to appear to be different than what it actually is. Instead of seeing the IP address 178.209.51.173 as the source of the attack, you would see, say, 64.4.11.37 – an address that has no connection to me at all.

IP spoofing is a well-known problem, and there are technical ways to prevent the basic kind of spoofing that just changes the IP address. However, there are also technical ways to *circumvent* the prevention mechanisms. More sophisticated prevention is then required to stop this, which again can be circumvented, etc. At the end of the day, IT security is an arms race between administrators trying to secure a network and potential attackers seeking to gain unauthorised access. But by the very design of the Internet, total security – including certainty of attribution – can never be achieved. As one introductory tutorial to IP spoofing put it, "IP Spoofing is a problem without an easy solution, since it's inherent to the design of the TCP/IP suite".[67]

Even more problematic than techniques such as IP spoofing is the use of "zombie" computers in cyber attacks. As outlined in the discussion of botnets above, cyber criminals and other attackers often use the machines and networks of unwitting third parties in their operations. These computer owners are usually not even aware that someone else has taken control of their computer and that they might be involved in an ongoing cyber attack. Graham Cluley, senior technology consultant at the IT security company Sophos, explained the problem as follows:

> Proving the origin of a hack attack is made more complicated by the fact that cybercriminals can use compromised PCs owned by innocent people to act as a go-between when trying to break into someone's computer. In other words – yes, a North Korean computer might have tried to connect to yours, but it may be under the control of someone in, say, Mexico.
>
> Denial-of-service attacks are relayed through innocent people's computers all around the world. Your Aunty Hilda's computer, which may normally be pumping out Viagra adverts, could today be engaged in a DDoS attack. In other words, innocent people's PCs may unwittingly be taking part in a cyber war.[68]

The series of DDoS attacks against US and South Korean websites in July 2009 are an excellent example of this. (See the detailed discussion in Chapter 5, p. 48 *ff.*)

Another showcase is the recently discovered malware *Flame*. Flame is a toolkit that allows the attacker to steal documents, capture login credentials, and even remotely turn on the internal microphone of an infected computer in order to eavesdrop on conversations. It is not known who is behind Flame, but due to its complexity security researchers have suggested that it might be a state-sponsored operation.[69] In any case, the machines from which the attackers controlled the infected computers were distributed around the world, including addresses in Germany, Poland, Malaysia, Latvia, Switzerland, Turkey, the Netherlands, the UK, and Hong Kong.[70]

The difficulty in establishing attribution has obvious consequences in the context of cyberwar. One crucial issue is the fact that attribution is a requirement before a response by armed force can be considered. (See the discussion of state responsibility in the analysis of the legal dimension of cyberwar, Chapter 4.) The strategic considerations are also significant. The difficulty of attribution invalidates traditional Cold War deterrence models, making it necessary to rather focus on defence and resilience. Former U.S. Deputy Secretary of Defense William J. Lynn III recognised this in outlining the Pentagon Cyberstrategy in 2010:

> Traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator. Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all. [...] The deterrence equation is further muddled by the fact that cyberattacks often originate from co-opted servers in neutral countries and that responses to them could have unintended consequences. Given these circumstances, deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation.[71]

Notes

[40] Brigid Grauman, "Cyber-security: The vexed questions of global rules", Report published by the Brussels think-tank *Security and Defense Agenda*, February 2012, `http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048`

[41] For a good introduction to the subject of botnets, see Ramneek Puri, "Bots & Botnet: An Overview.", *SANS Institute*, 8 August 2003, `http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299`

[42] Matthew Broersma, "Botnet price for hourly hire on par with cost of two pints", *ZDNet UK*, 25 May 2010, `http://www.zdnet.co.uk/news/security-threats/2010/05/25/botnet-price-for-hourly-hire-on-par-with-cost-of-two-pints-40089028/`

[43] Charles Clover, "Kremlin-backed group behind Estonia cyber blitz", *Financial Times*, 11 March 2009, `http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-`

0000779fd2ac.html

[44] Paul Wagenseil, "LulzSec Takes Down CIA Website ... On a Dare", *Security News Daily*, 15 June 2011, http://www.securitynewsdaily.com/778-lulzsec-takes-down-cia-website-on-dare.html

[45] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", *Schneier on Security*, 7 July 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html

[46] My colleague Thomas Steinbrenner once explain SQL injection in the following way: "Computers know two things: instructions and data. Simply speaking, an SQL injection is when the computer expects data as input but you provide instructions instead and trick it into executing them."

[47] An often cited example is an incident at Maroochy Water Services in Queensland, Australia, in the year 2000. A disgruntled ex-contractor manipulated a SCADA system to cause 800,000 liters of raw sewage to spill out, resulting in major environmental damage. For a detailed analysis of the incident, see Jill Slay and Michael Miller, *Lessons Learned from the Maroochy Water Breach* (Slay and Miller 2007).

[48] Éireann P. Leverett, *Quantitatively Assessing and Visualising Industrial System Attack Surfaces* (Leverett 2011).

[49] Kim Zetter, "10K Reasons to Worry About Critical Infrastructure", *Wired*, 24 January 2012, http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

[50] Thomas Rid, quoted in Anna Leach, "The cyber-weapons paradox: 'They're not that dangerous'", *The Register*, 24 February 2012, http://www.theregister.co.uk/2012/02/24/cyber_weapons/

[51] Thomas Rid, *Cyber War Will Not Take Place* (Rid 2012, p. 16).

[52] For a discussion of the legal and practical implications of applying the law of war rather than criminal statutes to prosecute terrorists, see Jennifer Elsea, "Terrorism and the Law of War: Trying Terrorists as War Criminals before Military Commissions", CRS Report RL31191, 11 December 2001, http://www.fas.org/irp/crs/RL31191.pdf

[53] Group-IB, "State and Trends of the Russian Digitial Crime Market", 24 April 2012, http://www.group-ib.com/index.php/7-novosti/630-russian-speaking-cybercriminals-earned-45-billion-in-2011-researchers-estimate

[54] Brigid Grauman, "Cyber-security: The vexed questions of global rules", report published by the Brussels think-tank *Security and Defense Agenda*, February 2012, http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048

[55] For a good portrait of Anonymous, see Nate Anderson, "Who Was That Masked Man?", *Foreign Policy*, 31 January 2012, http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man

[56] Peter Sommer, quoted in Eric Pfanner, "Apocalypse in Cyberspace? It's Overdone", *The New York Times*, 16 January 2011, http://www.nytimes.com/2011/01/17/technology/17cache.html?_r=1

[57] Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risk* (Sommer and Brown 2011, p. 81).

[58] (Rid 2012, p. 22)

[59](Rid 2012, p. 20)

[60]Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar* (Dunlap Jr. 2011, p. 84).

[61]Peter Sommer, quoted in Eric Pfanner, “Apocalypse in Cyberspace? It’s Overdone”.

[62](Rid 2012, p. 16)

[63]Irving Lachow, *Cyber Terrorism: Menace or Myth* (Lachov 2009, p. 448)

[64](Lachov 2009, p. 450)

[65]For a detailed analysis of the attribution problem, see Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (Brenner 2009, pp. 71–161).

[66]Not really.

[67]Matthew Tanase, “IP Spoofing: An Introduction”, *Symantec*, 11 March 2003, `http://www.symantec.com/connect/articles/ip-spoofing-introduction`

[68]Graham Cluley, “Is North Korea to blame for US cyber attacks?”, *Computerworld UK blog*, 9 July 2009, `http://blogs.computerworlduk.com/computerworld-archive/2009/07/is-north-korea-to-blame-for-us-cyber-attack/index.htm`

[69]Alexander Gostev, “Flame: Bunny, Frog, Munch and BeetleJuice..., *Securelist blog*, 29 May 2012, `http://www.securelist.com/en/blog/208193538/Flame_Bunny_Frog_Munch_and_BeetleJuice`

[70]Alexander Gostev, “The Roof Is on Fire: Tackling Flame’s C&C Servers”, *Securelist blog*, 4 June 2012, `http://www.securelist.com/en/blog/208193540/The_Roof_Is_on_Fire_Tackling_Flames_C_C_Server`

[71]William J. Lynn III, *Defending a New Domain. The Pentagon’s Cyberstrategy* (Lynn III 2010). Article also available online at the U.S. Department of Defense website, `http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx`

Chapter 4

Cyber Lawfare

This chapter presents the legal dimension of cyberwar, in particular the applicability of the law of armed conflict. Can a cyber incident constitute an attack that permits the victim state to respond by armed force, and how is cyber "force" to be seen in the context of a state of war?

The applicable law consists of two major sets of rules – the criteria for using force (formerly referred to as the *ius ad bellum*) and the law of armed conflict (previously called the *ius in bello*), which governs the behaviour of states and other subjects of international law during armed conflict. The following is an attempt to give an overview of how both sets of rules apply to cyber incidents.[72]

It should be noted that military cyber operations are not explicitly addressed under international law. Due to the relative novelty of the issue, state practice cannot be observed either. Lt. Gen. Keith B. Alexander, the first commander of the US Cyber Command, even warned Congress of a "mismatch between our technical capabilities to conduct operations and the governing laws and policies".[73] However, despite the fact that no explicit regulation exists, cyber attacks do not take place in a legal vacuum. They can and must be seen in the framework of existing international law.

4.1 The Prohibition of Force

Cyber attacks as armed attacks

For the purpose of this discussion, I will adopt the definition of computer network attacks given by the US Department of Defense, and define *cyber attacks* to be

> actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[74]

The first question that needs to be answered is whether a cyber attack can result in the right to an armed response on behalf of the attacked state. Article 2(4) of the UN Charter demands that:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.[75]

There are only two exceptions to the prohibition of the use of force: authorisation by the Security Council, and self-defence. With regard to self-defence, Article 51 of the UN Charter states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.[76]

Cyber operations may constitute a use of force prohibited by Art. 2(4). Whether a particular incident qualifies as such an act has to be determined on a case-by-case basis. To do this, the effects of the cyber attack have to be assessed. Michael N. Schmitt, Chairman of the International Law Department at the United States Naval War College, proposed seven factors that must be evaluated to determine whether a particular cyber operation amounts to the use of force. These factors are severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[77]

Even cyber attacks that constitute a prohibited use of force do not automatically allow for an armed response. It is important to note that Article 2 prohibits all threats and use of "force", while Article 51 speaks of a *specific* kind of force, namely an "armed attack". This distinction is important.[78] A use of force short of an "armed attack" still allows the victim state to respond by other means, such as the unilateral severance of economic and diplomatic relations, civil lawsuits, and application to the UN Security Council. It does not, however, permit recourse to the use of force.[79]

Under what circumstances then might a cyber attack qualify as an armed attack?

Article 49 of Protocol I to the Geneva Conventions defines attacks to mean "acts of violence against an adversary".[80] Such acts of violence need not necessarily be of a kinetic nature. Rather, their *consequences* have to be analysed. A parallel can be drawn here to the treatment of biological and chemical weapons under international law. These weapons are not kinetic in nature, but due to their harmful effects on human beings, their utilisation is considered to amount to armed force.[81] Similarly, even though a cyber attack is not kinetic in itself, it may inflict damage comparable to that of a kinetic weapon, and thus constitute an act of violence in the sense of the definition above. An example for this would be a SCADA attack that destroys an industrial facility. (See p. 19 for a technical definition of SCADA systems.)

It would thus have to be shown that the effects of a cyber attack amount to the equivalent of an armed attack before the right to self-defence can be invoked. In particular, the consequences must be more than mere inconvenience:

> The essence of an “armed” operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects.[82]

A cyber attack only constitutes an armed attack in the sense of the UN Charter if this level of violence is met. Clearly, the majority of cyber incidents fall far short of this threshold.

State responsibility

It is important to keep in mind that the law of armed conflict governs relations between states, not individuals. Thus it becomes an essential question if and under what circumstances a cyber attack can be attributed to a state. This problem of attribution is, as Navy Judge Advocate General Todd C. Huntley put it, “the single greatest challenge to the application of the law of armed conflict to cyber activity”.[83]

In general, under international law the conduct of private actors is not attributable to a state. The General Counsel of the US Department of Defense acknowledged this as relevant in the context of information operations:

> When individuals carry out malicious [cyber] acts for private purposes, the aggrieved state does not generally have the right to use force in self-defense.[84]

Under what circumstances can a state be held responsible for the actions of private actors? The International Court of Justice ruled on this in the *Nicaragua* case, finding that for a state “to be legally responsible, it would have to be proved that that State had effective control of the operations [of the private actors]”.[85] The International Criminal Tribunal for the former Yugoslavia (ICTY) established a similar, if somewhat lower, threshold for imputing private acts to states in the *Tadic* case. The ICTY concluded that a state only need to exercise “overall control” [rather than “effective control”] over private actors in order for their unlawful acts to be attributable to the state.[86]

The imputation of state responsibility thus requires some form of *effective or overall control* by the state over the private actors. Establishing this is particularly difficult in the case of cyber attacks, not least due to the technical problems of discovering the identity of an attacker in the first place. (See also the technical remarks on attribution in Chapter 3, p. 24 *ff.*)

When such control over non-state actors cannot be established, the responsibility of the state is limited to exercising *due diligence*, which means that the state must take all “reasonable” and “necessary” measures in order to prevent a given incident from happening – however without a warranty that it will not occur. What exactly this means in the context of cyber operations remains unclear.[87]

4.2 The Law of Armed Conflict

Whether incidents should be treated as the actions of belligerents under the law of armed conflict or as the actions of individuals that may be subject to the rules of (civilian) law enforcement depends on the presence (or absence) of a state of armed conflict.

However, determining whether a state of armed conflict exists is not always obvious, and there are various (and conflicting) interpretations. It should be noted that neither a formal declaration of war nor the recognition of a state of war are necessary preconditions. Yoram Dinstein, former President and Dean of Law at Tel Aviv University, defines war to be:

> a hostile interaction between two or more States, either in a technical or in a material sense. War in the technical sense is a formal status produced by a declaration of war. War in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.[88]

The key terms here are *“States”*, *“armed force”*, and *“comprehensive”*. As Schmitt points out, “cyber violence of any intensity engaged in by isolated individuals or by unorganized mobs, even if directed against the government" does not create a situation to which the law of armed conflict applies.[89]

It seems unlikely that a state of armed conflict can arise from the use of cyber attacks alone. (My reasons for making this assertion are explained in detail in Chapter 7.) However, clearly military cyber operations will play a role in future conflicts, making it interesting to consider how these new cyber "weapons" will have to be seen in the context of the law of armed conflict.[90]

Applicability of the law of armed conflict to military cyber operations

First of all, it is clear that the basic principles of the law of armed conflict apply also to cyber operations. If a state of armed conflict exists, cyber "weapons" must be employed in a manner consistent with the relevant laws. As stated in Article 36 of Protocol I to the Geneva Conventions:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[91]

The basic principles that have to be observed include the principle of *distinction* and the principle of *proportionality*. The principle of distinction requires that attacks be limited to military objectives, and that civilians or civilian objects must not be targeted. The principle of proportionality prohibits attacks that might kill or injure civilians or cause damage to civilian objects if these attacks "would be excessive in relation to the concrete and direct military advantage anticipated".[92]

While there is no doubt that the law of armed conflict applies to military cyber operations, it is not always immediately clear how the existing rules are to be interpreted in this context. It is not possible to give a comprehensive analysis here, but I want to briefly discuss four specific issues that show the kinds of questions that are raised, and how these questions can be dealt with by way of analogy to non-cyber situations.

Civilian participation in cyber hostilities

One interesting issue is the question of civilian participation in armed conflict in the context of cyber operations.[93] The lines become much more blurred than with traditional fighting. Are civilians that engage in acts of "patriotic hacking" to be seen as taking an active part in the hostilities?

Johann-Christoph Woltag, Research Fellow at the Max Planck Institute for Comparative Public Law and International Law, argues that the answer depends on the degree of harm that is inflicted and on the causal proximity to the target. In this sense, it seems that typical harmful cyber activities such as DDoS attacks or website defacements would not qualify:

> Depriving the enemy of intangible assets such as bank accounts lacks the necessary nexus to the battlefield and can thus not be regarded as active participation. The same must then hold true for less drastic acts such as website defacements and the like. [...] A large number of DDoS may cause the internet infrastructure to be unavailable, as seen in Estonia. Nevertheless, the level of harm done by one individual remains rather low also in this case, posing difficulties to establishing the threshold needed to qualify the attack as participation.[94]

The legality of spoofing

It is easy to mask the origin of a cyber attack and thus conceal the attacker's identity by "spoofing" its origin. (For a technical explanation, see p. 24 *ff.*) A spoofed attack may appear to originate from a civilian computer system or from a computer system belonging to the military of a neutral state. As a consequence, this third-party system may then be targeted by the opponent. Is such a practice legal under international law?

In order to protect civilians from the effects of armed conflict, Article 37(1) Additional Protocol I prohibits acts of perfidy:

> It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy.[95]

Art. 37(1)(c) explicitly lists "the feigning of civilian, non-combatant status" as an example of prohibited perfidy. It can be argued that, depending on the circumstances, masking the origin of an attack has to be regarded as an illegal perfidious act in this sense. However, this only applies if the act in question results in the killing, injury or capture of an adversary. This leaves a wide range of possibilities where it would be legal for the armed forces to use spoofing.[96]

Civilian-military interdependence and the principle of distinction

Military cyber operations are likely to make use of the public Internet. At the same time, civilians are using (and are in some sense even depending on) the global network. Is it legal to target the Internet, i.e. the physical infrastructure that sustains the network, such as public Internet Service Providers (ISPs), data centres, and so on? Article 52(2) Additional Protocol 1 states that:

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to 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 of advantage.[97]

However, under the law of armed conflict, *dual-use objects* that serve both civilian and military purposes may be legitimate military objectives. If the armed forces make use of the civilian network infrastructure, the Internet has to be seen as a dual-use object. As with any dual-use object, Internet infrastructure may thus be considered a military objective, if the two criteria of Art. 52(2) – *effective contribution to military action* and *definite military advantage* – are fulfilled.

The principle is distinction also has interesting consequences regarding the kinds of cyber attacks that may be legally employed. Indiscriminate attacks are prohibited, so an attack that targets a specific military computer system would be legal – but a computer virus that spreads uncontrollably among military as well as civilian computer systems or networks would not be allowed.

Transboundary data transmission and neutrality

The fundamental protocols that define data transfer on the Internet invariably result in transboundary data transmission. In most cases data transferred (in technical terms: "routed") between two points will cross several territorial jurisdictions on its way. This raises the question of whether such a transmission violates the neutrality of third states during armed conflict.

Suppose that state A launches a cyber attack against state B. From a technical perspective, the attack consists of a series of IP packets that are transferred from a computer system in A to a computer system in B by way of the public Internet. On their way, these packets cross through the territory of neutral state C. Does this transmission violate C's neutrality?

Two interpretations are possible. One would be to equate the routing of the packets with the movement of troops or munitions through C's territory, which would be a violation of the Hague Convention V on the Rights and Duties of Neutral Powers and Persons. Article 2 Hague Convention V states that

> Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.[98]

Another interpretation would be to draw an analogy between the routing of data and the use of telephone cables by belligerents, which is not prohibited. As Article 8 Hague Convention V makes clear:

> A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.[99]

I tend towards the latter reading, taking Art. 8 to refer to telecommunications infrastructure in general. The routing of packets through C's Internet infrastructure would thus be a legal use thereof.

This question is important since neutral states are obliged to suppress belligerent activity on their territory (insofar as they are capable of doing so). If data transmission was equated with troop movements, neutrals would have to take measures to stop it. However, this would be practically impossible and require the state to monitor all Internet activity across their territory.

A different situation arises when a cyber attack is launched from a computer on the neutral state's territory. This could potentially induce the attacked state to falsely attribute the attack to the neutral state and launch a counter-attack. In addition to potentially being prohibited as an act of perfidy (see above), this would clearly also be a violation of the neutrality of the neutral state.[100]

4.3 Cybercrime, Not Cyberwar

With the potential exception of the Stuxnet incident (see Chapter 6), none of the cyber attacks that have been observed to date reach the threshold of armed force as outlined above. Therefore these incidents are not acts of "cyberwar" to which the law of armed conflict applies. They are properly dealt with using applicable national and international criminal law.

Let me underline that even though contemporary cyber attacks do not fall into the domain of armed conflict, they do have relevance in the context of international security. State actors might even have an incentive to specifically resort to cyber attacks that stay below the threshold of armed force. As a 2008 report by the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn warned,

> From a legal point of view, given the current and projected future threat environment (increasing threat of asymmetric attacks by non-state entities, less threat of state-sponsored warfare), there is an increasing likelihood of "grey area" attacks. In fact, it is the general murkiness of this grey area – the lack of clear policies and procedures, the lack of direct evidence of the attacking entity's identity – that may make such "grey area" attacks even more attractive. In such a perceived environment, by deliberately remaining below the threshold of "use of force," an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected.[101]

This makes it all the more important to establish international cooperation to deal with these attacks – as potentially criminal acts, not acts of (cyber) warfare.

A detailed analysis of the possibilities and limitations of efforts to address cybercrime would be beyond the scope of this thesis. Suffice it to say that the first steps in the right direction have already been made, though clearly much remains to be done. The first international instrument addressing cybercrime – the Convention on Cybercrime – was adopted by the Council of Europe in 2001 and entered into force in July 2004.[102] The convention provides guidelines for states to develop comprehensive national legislation against cybercrime and establishes a framework for international cooperation in the investigation of cybercrimes. Accession by non-European states is possible and encouraged. To date, thirty-three states have ratified the cybercrime convention, including most EU countries and the United States. Unfortunately, some of the states from which the majority of cyber attacks appear to originate have not yet acceded to the convention, limiting its usefulness in international cooperation. Russia in particular has announced its intent not to ratify the convention, which it claims might "damage the sovereignty and security of member countries and their citizens' rights".[103]

In conclusion, it should be noted that the legal questions raised in this chapter are not merely of academic interest. They are of crucial practical significance, since they determine the appropriate response to a cyber attack. As Charles J. Dunlap Jr. points out,

> This is a distinction with a difference. A national-security legal regime is one where LOAC largely governs, while the law enforcement model essentially employs the jurisprudence of criminal law. The former is inclined to think in terms of eliminating threats through the use of force; the latter uses force only to contain alleged lawbreakers until a judicial forum can determine personal culpability. An action legitimately in the realm of national security law may be intolerant of any injury and, when hostile intent is perceived, may authorize a strike to prevent it from occurring. Law enforcement constructs presume the innocence of suspects and endure the losses that forbearance in the name of legal process occasionally imposes.[104]

If the applicability of the law of armed conflict cannot be established, a cyber attack must be treated as a matter of law enforcement:

> As a matter of legal interpretation, nation-states do not wage war against criminals; rather, they conduct law enforcement operations against them.[105]

The appropriate legal concept for dealing with the vast majority of cyber attacks is thus cybercrime, not cyberwar.

Notes

[72] For a more comprehensive analysis, see e.g. (Huntley 2010).

[73] Thom Shanker, "Cyberwar Nominee Sees Gaps in Law", *The New York Times*, 14 April 2010, `http://www.nytimes.com/2010/04/15/world/15military.html`

[74] US Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations", 13 February 2006, `http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf`

[75] Charter of the United Nations and Statute of the International Court of Justice, 1945, `http://treaties.un.org/doc/Publication/CTC/uncharter.pdf`

[76] *ibid.*

[77] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts* (Schmitt 2010).

[78] All armed attacks are uses of force within the meaning of Article 2, but not all uses of force qualify as armed attacks that permit a response of self-defense. See also (Schmitt 2010).

[79] Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar* (Dunlap Jr. 2011).

[80] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 8 June 1977, `http://www2.ohchr.org/english/law/protocol1.htm` – from here on referred to as *Additional Protocol I*.

[81] Johann-Christoph Woltag, *Cyber Warfare* (Woltag 2010).

[82] (Schmitt 2010, p. 163)

[83] Todd C. Huntley, *Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare* (Huntley 2010, p. 34).

[84] Office of General Counsel, "An Assessment of International Legal Issues in Information Operations", November 1999, `http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc`

[85] ICJ, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", Judgment of 27 June 1986, `http://www.icj-cij.org/docket/index.php?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5`. See also (Jinks 2003, p. 88)

[86] ICTY, "Prosecutor v. Tadic (Case No. IT-94-1-A)", Judgment of 15 July 1999, `http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf`.

The imputation of State responsibilty remains a contested question, as can be most clearly seen by the response of the international community to the United States' *Operation Enduring Freedom* in 2001. The US justified its invasion of Afghanistan by the fact that the Taliban regime had harboured and supported Al Qaeda. The Taliban did likely not exercise effective or overall control over the terrorist group's operations, but this did not stop the US and its allies from starting armed operations in Afghanistan in what they considered an act of self-defense. See also (Jinks 2003, pp .85–87).

[87] For an analysis of how the principle of due diligence may apply to cyber attacks, see Joanna Kulesza, *State Responsibility for Cyberattacks on International Peace and Security* (Kulesza 2009).

[88] Yoram Dinstein, *War, Aggression and Self-Defence* (Dinstein 2005, p. 15).

[89] (Schmitt 2010, p. 175)

[90] It should be noted that the notion of what constitutes a cyber "weapon" is in itself not clear. See Thomas Rid and Peter McBurney, *Cyber-Weapons* (Rid and McBurney 2012).

[91] Additional Protocol I

[92] Harold Hongju Koh, “The Obama Administration and International Law”, speech at the Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010, http://www.state.gov/s/l/releases/remarks/139119.htm

[93] For a detailed analysis of the difficulty of separating between combatants and noncombatants in a “cyberwar” context, see Susan W. Brenner and Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts* (Brenner and Clarke 2010).

[94] (Woltag 2010)

[95] Additional Protocol I

[96] (Woltag 2010)

[97] Additional Protocol I

[98] Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, http://www.unhcr.org/refworld/docid/3ddca4e14.html

[99] Hague Convention (V)

[100] (Woltag 2010)

[101] Eneken Tikk et al, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tikk et al. 2008, p. 29).

[102] Council of Europe, *Convention on Cybercrime*, CETS No: 185, November 2001, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

[103] “Putin defies Convention on Cybercrime”, *Computer Crime Research Center*, 28 March 2008, http://www.crime-research.org/news/28.03.2008/3277/

[104] (Dunlap Jr. 2011, p. 84)

[105] (Dunlap Jr. 2011, p. 88)

Chapter 5

Cyberwar Story Time

This chapter describes a number of incidents that are widely cited as examples of cyberwar. I will attempt to clearly present what is actually known about each of these events, and to distinguish fact from fiction, showing to what degree the label of cyberwar is appropriate in each case.

5.1 The Farewell Dossier

In June 1982, a natural gas pipeline in Siberia blew up in a "the most monumental nonnuclear explosion and fire ever seen from space".[106] This explosion, estimated by the U.S. Air Force at 3 kilotons – equivalent to a small nuclear device – was caused by a "logic bomb" embedded in the control system software that the Soviets had stolen from Canada, making the blast the most devastating cyber attack to date.

Or so the story goes.

Thomas C. Reed, President Reagon's special assistant for National Security Policy at the time, recounts the tale in his 2004 book, *At the Abyss: An Insider's History of the Cold War*.[107] In the early 1980s, there was a concerted effort by the KGB's Technology Directorate to acquire – and if necessary, steal – Western technology. The extent of Soviet penetration into U.S. and other Western laboratories, factories and government agencies was revealed in the *Farewell Dossier*, a collection of documents leaked to the French *Direction de la Surveillance du Territoire* (DST) by a defected KGB agent, Colonel Vladimir I. Vetrov, codenamed "Farewell".[108] The dossier contained not only the names of KGB double agents in the Western world but also the "shopping list" for military and industrial technology to acquire – legally or illegally – during the coming years. The DST shared this dossier with the CIA, which saw a golden opportunity to do massive damage to the Soviet economy. As Gus W. Weiss, Director of International Economics for the National Security Council at the time, recounts:

> I proposed using the Farewell material to feed or play back the products sought by Line X [the KGB's Technology Directorate's operational arm], but these would come from our own sources and would have been "improved," that is, designed so that on arrival in the Soviet Union they would appear genuine but would later fail. US intelligence would match Line X requirements supplied through Vetrov with our version of those items, ones that would hardly meet the expectations of that vast Soviet apparatus deployed to collect them.[109]

In other words, the U.S. would allow the Soviet technology acquisition programme to go forward, but the computer chips and software were modified to contain "logic bombs" – intentional hidden flaws that would cause damage by changing their proper operation.

One of the pieces of technology that the Soviets sought to acquire was for a new trans-Siberian pipeline delivering natural gas from the Urengoi gas field in Siberia to the West. They needed an industrial control system to automate the pipeline's operation of valves, compressors and storage facilities. Eventually they succeeded in obtaining the necessary hardware and software from Canada – but what they received was a Trojan horse. In order to convince the operators that the new system was working well, the pipeline control software was programmed to operate as intended at first. However, after a while, it would produce erratic output, resetting pump speeds and valve pressures far outside the acceptable operating parameters. This is allegedly what caused the explosion in June 1982.[110]

It is an intriguing tale, but did it really happen? There are three indications that shed doubt on the veracity of the story. First, there are no media reports from 1982 that mention the explosion. The only source for this story appears to be Thomas Reed's book – even though other pipeline accidents that happened in the Soviet Union at the time were regularly reported. Secondly, Vasily Pchelintsev, a former KGB officer from the Tyumen region where the explosion allegedly took place, denied that the incident described by Reed took place.[111] Admittedly, the KGB might be reluctant to admit to having been duped. On the other hand, the Soviet Union has acknowledged the existence of the Farewell dossier – and executed Colonel Vetrov for his espionage activities in 1983. If a massive pipeline explosion had taken place, would it not be better to blame it on U.S. sabotage rather than admitting embarrassing technical failure? Thirdly, even though the CIA acknowledged the large-scale deception operation to supply the Soviet Union with defective technology, including such operational successes as the failure of the Soviet Space Shuttle programme, it did not mention the 1982 explosion at all.[112]

The only evidence for this incident is thus Thomas Reed's account. Reed himself was not involved in the project but claims to have learnt about it more than twenty years later when doing research for his book. Therefore, I would hesitate to count this supposed pipeline explosion as a proven case of a successful cyber attack that caused real-world damage.

5.2 Web War One

A series of distributed denial-of-service attacks (see p. 16 *ff.* for a technical explanation) hit a number of websites in Estonia during a three-week period in April and May 2007. Affected websites included the Estonian parliament and several ministries, banks, and news outlets. More than 85,000 computers were involved in the attacks. The peak of the attacks was reached on 9 May 2007, when fifty-eight Estonian websites were inaccessible, including Estonia's largest bank. The sources of the DDoS attacks were distributed world-wide, according to Jose Nazario, an IT security researcher at *Arbor Networks* who studied the incident in detail. Attack bandwidths ranged mostly from 10 to 30 Mbps, with peaks up to 95 Mbps. Most attacks were short term – three quarters of them did not last longer than one hour, and only 5.5 percent succeeded in making a site inaccessible for more than ten hours.[113]

The DDoS attacks appear to be linked to Estonian plans to relocate the *Bronze Soldier*, a World War Two memorial commemorating the Russian soldiers who died in the liberation of Tallinn. The statue was to be moved from the city centre to a cemetery in the suburbs. Many ethnic Russians living in Estonia were outraged at what they saw as a slight to the memory of their fallen compatriots. The memorial's removal was followed by riots in Tallinn during which one person was killed and more than 150 were injured.[114]

The Estonian DDos attacks were widely reported in the media as being the first cyberwar. The term *Web War One* was coined – and used in a non-ironic way – to refer to the incident.[115] Estonian Prime Minister Andrus Ansip directly accused the Russian Federation of being responsible for the DDoS attacks. Ansip compared the DDoS attacks to a naval blockade, asking rhetorically:

> What is the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?[116]

The Speaker of the Estonian Parliament, Ene Ergma, went even further:

> When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing.[117]

Despite this warlike rhetoric, the DDoS attacks on Estonian websites do *not* constitute an act of war. There was no effect other than a few websites being temporarily inaccessible. In other words, the attacks caused inconvenience (and maybe some financial loss), but they were not violent in nature. Prime Minister Ansip's analogy between DDoS attacks and a naval blockage is deeply flawed: A blockade is inherently based on the use of physical force or the threat thereof, preventing ships from entering or leaving an area *by force* if necessary. No such force was used in temporarily impeding access to the Estonian websites. As for Ene Ergma's remarks, I am not quite sure what "explosion" she refers to, but again, clearly DDoS attacks are certainly not equivalent to a nuclear explosion.

Besides not being violent, the attacks were also not attributable to a state actor, in this case Russia. Rather, data gathered by Arbor Networks indicates that the attacks appear to be the "spontaneous product of a loose federation of separate attackers". As Jose Nazario concluded:

> So, we see signs of Russian nationalism at work here, but no Russian government connection. None of the sources we have analyzed from around the world show a clear line from Moscow to Tallinn; instead, it's from everywhere around the world to Estonia.[118]

Security expert Bruce Schneier agrees:

> The attacks against Estonian websites in 2007 were simple hacking attacks by ethnic Russians angry at anti-Russian policies; these were denial-of-service attacks, a normal risk in cyberspace and hardly unprecedented.[119]

This analysis is generally accepted in the information security community today. Even Estonia has by now formally withdrawn the cyberwar accusations against Russia, relabelling the attacks as "criminal activity" and asking for help from Russia in their investigation to find the actual perpetrators behind the attacks. In the words of Prime Minister Ansip: “It is clear this is criminal activity. I hope Russia will co-operate in those cases with Estonia.”[120]

Even so, the Estonian case continues to be widely cited as the first cyberwar – despite all the evidence to the contrary.

5.3 Cyber War 2.0

On 8 August 2008, the Russian Federation launched a five-day military campaign against Georgia in response to Georgia’s attempts to assert greater control over Abkhazia and South Ossetia, regions with a strong ethnic Russian population. At the same time, a wave of cyber attacks hit Georgian government, media, and banking websites, including the websites of Georgia’s President Mikhail Saakashvili, the Defense Ministry, and the National Bank of Georgia.[121]

As in the Estonian case a year earlier, the majority of attacks were distributed denial-of-service attacks aiming at making websites in the public and private sector inaccessible. These DDoS attacks lasted on average around 2 hours and 15 minutes. The longest time that a single site was offline was less than six hours. The attacks had a much higher intensity than the ones observed in Estonia, with a traffic average of 211.66 Mbps and reaching a peak at 814.33 Mbps.[122]

In addition to the DDoS attacks, a number of websites were defaced as well (see p. 18 *ff.* for a technical explanation). The most prominent of these acts of online vandalism was conducted by a group calling itself the *South Ossetia Hack Crew*. Members of the group gained access to the website of the Georgian Parliament on 11 August 2008 and posted a collage of pictures of Adolf Hitler and Mikhail Saakashvili under the headline *“Find 10 differences. Find your ruler.”*

An interesting feature of the Georgian case was the proliferation of special malware packages that would allow individuals to join the attacks. A forum called *StopGeorgia.ru* was created on 9 August 2008, a day after the start of Russia’s military campaign against Georgia. The purpose of the forum was to coordinate attacks on 37 high-profile websites in Georgia. The administrators of the forum provided members with downloadable DDoS kits – one of which was adequately named *war.rar* – as well as giving advice on how to launch more sophisticated attacks.[123]

As in the Estonian case, the media was quick to call these attacks a cyberwar. Following *Web War One* in Estonia in 2007, this new war was dubbed *Cyber War 2.0*.[124]

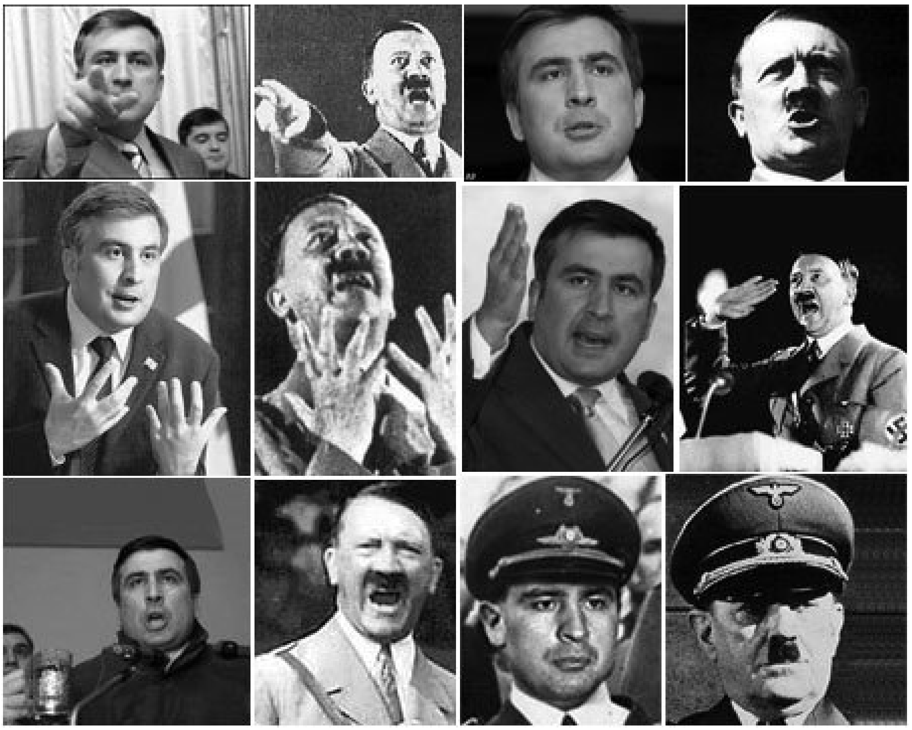

Figure 3: Georgian Parliament website defaced.

Were these cyber attacks related to Russia's military campaign? Undoubtedly. The question is to what degree the Russian Federation as a state can be connected to the attacks. From the technical data, it is impossible to say. Officially, Russia has denied all involvement. In fact, it is much more likely that, as in Estonia, the wave of cyber attacks were the work of individuals rather than part of an organised effort.

Gadi Evron, an expert on Internet security and founder of the Israeli Government CERT, cautioned against "pointing fingers" without evidence:

> Until we are certain anything state-sponsored is happening on the Internet it is my official opinion this is not warfare, but just some unaffiliated attacks by Russian hackers and/or some rioting by enthusiastic Russian supporters. [...] It is simply too early and there is not enough information to call this an Internet war. [...]
>
> Following any political or ethnic tension, an online aftermath comes in the form of attacks, defacements, and enthusiast hackers swearing at the other side (which soon does the same, back). From a comic of the Prophet Muhammad to the war in Iraq, the Internet has given people a voice, even if sometimes expressed in irrational ways. [125]

Evron further argues that if Russia had been behind this campaign, the attacks would likely have been much more serious and targeted towards critical infrastructure, rather than just causing some inconvenience and embarrassment:

> Food for thought: Considering Russia was past playing nice and used real bombs, they could have attacked more strategic targets or eliminated the infrastructure kinetically.[126]

An in-depth report compiled by the U.S. Cyber Consequences Unit, an independent nonprofit research institute that assesses the impact of cyber attacks, suggests the same:

> Investigations by the US-CCU suggested that a number of Georgian critical infrastructures were accessible over the internet at the time Russia invaded Georgia. There is reason to believe that at least some of these infrastructures would have been vulnerable to cyber attacks causing physical damage. [...] If the Russian military had chosen to get directly involved, such attacks would have been well within their capabilities.[127]

Of course, saying that the cyber attacks were not conducted directly by the Russian military does not mean that they were not beneficial to the war. Scott Borg, Director and Chief Economist of the U.S. Cyber Consequences Unit, pointed out that there was likely some level of interaction between organised criminal groups involved in the cyber attacks and the Russian government. According to Borg, Russia "appeared to be leveraging civilian nationalists who were ready to take cyber action, perhaps with some low-level encouragement. It appears that the military invasion was taking into account the help they were about to receive by the cyberattack".[128]

The fact that a cyber attack benefits an ongoing actual war or may happen with the encouragement or even support of the armed forces does not make it into an act of war though. Going back to the definition suggested in the introduction, the first criteria for an act of war has to be that it is actually or at least potentially *violent* – which, as explained above, does not apply to DDoS attacks and website defacements. An analysis on the legal lessons of the Georgian cyber attacks published by the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia came to the same conclusion:

> It is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect.[129]

Therefore, as with the Estonian case a year earlier, and despite widespread assertions to the contrary, what happened in Georgia in August 2008 was *not* a cyberwar.

5.4 From Pyongyang With Love?

On the weekend of the Fourth of July 2009, a series of DDoS attacks targeted various US websites, including the White House, the Federal Trade Commission, the New York Stock Exchange and NASDAQ.[130] A couple of days later, DDoS attacks also hit a number of South Korean targets, including the websites of South Korea's president, the Blue House, and the National Assembly, as well as major banks such as Shinhan Bank and Korea Exchange Bank.[131]

As has been explained in the cases of Estonia and Georgia above, DDoS does not constitute an act of (cyber) war, since the attacks have to be seen as mere inconvenience not causing any lasting damage beyond potential financial loss.[132] What makes these attacks interesting – and the reason I am discussing them here – is that they provide an excellent example of the difficulty of attribution.

American representatives were quick to put the blame on the Democratic People's Republic of Korea. Senator Peter Hoekstra told the *Washington Times'* radio programme that the attacks were state-sponsored and that "all fingers point to North Korea." He urged the US to send a strong message, warning that North Korea could go on to shut down the banking system or interfere with the electrical grid and "people could be killed".[133]

There was little evidence though that these allegations were true. In fact, it turned out that the attack utilised a very large number of computers distributed around the world that had been infected with a virus. Nguyen Minh Duc, senior security director at Bach Khoa Internetwork Security Centre (Bkis), reported that 166,908 infected computers in 74 countries were involved in the attack. The largest number of infected PCs were in South Korea, followed by the US, China, Japan, Canada, Australia, the Philippines, New Zealand, the UK and Vietnam.[134] The master command-and-control server – the machine used to coordinate the DDoS attacks – was using an IP address belonging to a company based in Brighton in the UK. Further investigation showed that the server itself was actually located in Miami, Florida.[135]

To date, it is not known who was behind the series of DDoS attacks on US and South Korean websites. The company owning the command-and-control server in Miami has acknowledged that they found "viruses" on the computer and that they are "doing an investigation internally”, but no outcome of that investigation has been made publicly available.[136] It is unlikely that there will be any conclusive results. If anything, the case of the July Fourth attacks shows the difficulty of establishing attribution.

What to make of an attack run by 166,908 computers in 74 countries, coordinated from a machine in Miami that is logically based in the UK? The main lesson that can be drawn from the incident is that one should be cautious about assigning blame without evidence. Graham Cluley, senior technology consultant at the IT security company Sophos, warned about this in a blog post published just days after the DDoS attacks started:

> Fingers have inevitably been pointed at the government of North Korea. [...] But is it as simple as that? What is still lacking is any evidence proving that the distributed denial-of-service attacks are backed by the Korean government or military rather than the work of independent hackers.
>
> A single hacker in a back bedroom can command a botnet of thousands of computers to bombard a website with traffic (a denial of service attack, causing the site to effectively fall off the net for a while). So there’s no reason why a government or army couldn’t do the same thing. The thing is, it’s very hard to *prove* that an attack is officially sponsored by a particular government or army rather than a lone individual or hackivist with an axe to grind. [...]
>
> We’d be naive to think that North Korea (and just about every other country around the world) isn’t using the internet for its political, commercial and military advantage, but we should be very cautious about making accusations without having all the evidence in front of us.[137]

5.5 Operation Aurora

Operation Aurora[138] was a cyber attack against Google and at least twenty other companies in the second half of 2009. The attack used a zero-day vulnerability in Microsoft Internet Explorer to install malware on the target computers. This malicious program then copied confidential data to a remote system.[139] Operation Aurora was discovered in January 2010, when Google published a blog post stating that

> In mid-December, we detected a highly sophisticated and targeted attack

> on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google.[140]

In addition to Google, other companies that were targeted included Adobe Systems, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical.[141] According to researchers at IT security company McAfee who analysed the Operation Aurora attacks, the primary goal was to gain access to the main source code repositories of these companies:

> [The source code repositories] were wide open. No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways – much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting.[142]

Security experts agree that the attack was unusually sophisticated. There also seems to be little doubt that the attack did, in fact, originate from China.[143] Does this make Operation Aurora into an act of cyberwar though?

In a statement issued two weeks after the incident became public, China officially denied any involvement. A spokesperson from the Ministry of Industry and Information Technology stated that

> Accusation that the Chinese government participated in cyber attack, either in an explicit or inexplicit way, is groundless and aims to denigrate China. We [are] firmly opposed to that.[144]

A leaked diplomatic cable from the US Embassy in Beijing, however, seemed to suggest state involvement. The New York Times, who had full access to the cables released by Wikileaks, reported in November 2010:

> China's Politburo directed the intrusion into Google's computer systems in that country, a Chinese contact told the American Embassy in Beijing in January, one cable reported. The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and Internet outlaws recruited by the Chinese government. They have broken into American government computers and those of Western allies, the Dalai Lama and American businesses since 2002, cables said.[145]

The question remains, of course, to what degree this statement can be taken at face value. The global headlines that followed, such as *WikiLeaked diplomatic cables confirm China's Politburo was behind Google hacking incident*, seem a bit premature, to say the least.[146] "Confirm" certainly is too strong a word. The cable cites an unknown source who claims to know that "someone" in the Politburo ordered the attacks. We do not know who that source was, if they were in a position to know, or how seriously the US embassy in Beijing took the information. Thus this leaked diplomatic communication certainly provides an interesting perspective, but I would be wary about treating them in any way as confirmation.[147]

In any case, even if Chinese state involvement could be proved, the objective of Operation Aurora was to steal intellectual property. To what degree the attackers succeeded to do this remains unclear, but even if they did, no physical damage resulted from the attack. Thus, however Operation Aurora has to be evaluated in the light of US-China relations, it clearly was not an act of (cyber) war.

5.6 Operation Orchard

Unlike the other stories discussed in this chapter, Operation Orchard is rarely mentioned in the context of cyberwar. However, unlike these other incidents, Operation Orchard is a real-life example of how information technology can actually play a significant role in military operations.

On 6 September 2007, the Israeli Air Force conducted a bombing raid on an alleged nuclear reactor site at Al-Kibar near Deir ez-Zor in northern Syria. Apparently an entire Israeli squadron of F-15I and F-16I warplanes was able to enter the Syrian airspace, raid the site, and leave, without any response from Syrian air defence.[148]

The details of Operation Orchard remain classified. But it has been speculated that the Israelis used a "kill switch" in the Syrian radar system to temporarily interfere with its operation:

> Among the many mysteries still surrounding that strike was the failure of a Syrian radar – supposedly state-of-the-art – to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare – and not just any kind. Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated

> with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar.[149]

Given the dearth of public information about Operation Orchard, it is hard to say whether this speculation is true. Satellite images have confirmed, though, that the attack on the Al-Kibar facility did indeed take place, and it did not provoke any response from the Syrian air defence. This suggests that *some* kind of interference with the defence system must have taken place. Therefore, Operation Orchard stands as one example where a cyber attack probably played a crucial role in a military operation. As Thomas Rid has analysed,

> The cyber element of Operation 'Orchard' probably was critical for the success of the Israeli raid and although the cyber attack did not physically destroy anything on its own right, it should be seen as an integrated part of a larger military operation. Although the cyber attack on its own – without the military component – would not have constituted an act of war, it was nevertheless an enabler for a successful military attack.[150]

It is Operation Orchard, rather than *Web War One*, that we should look towards as foreshadowing the future significance of military cyber operations.

Notes

[106] Matthew French, "Tech sabotage during the Cold War", *Federal Computer Week*, 26 April 2004, `http://fcw.com/Articles/2004/04/26/Tech-sabotage-during-the-Cold-War.aspx`

[107] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Reed 2004).

[108] For a comprehensive (and highly intriguing) account of the Farewell affair, see Sergei Kostine and Eric Raynaud, *Adieu Farewell* (Kostine and Raynaud 2009).

[109] Gus W. Weiss, *The Farewell Dossier* (Weiss 1996, p. 124).

[110] Matthew French, "Tech sabotage during the Cold War".

[111] Anatoly Medetsky, "KGB Veteran Denies CIA Caused '82 Blast", *The Moscow Times*, 18 March 2004, `http://www.themoscowtimes.com/news/article/kgb-veteran-denies-cia-caused-82-blast/232261.html`

[112] (Weiss 1996)

[113] "Estonian DDoS - a final analysis", *Heise Online*, 31 May 2007, `http://www.h-online.com/security/news/item/Estonian-DDoS-a-final-analysis-732971.html`

[114] "Estonia hit by 'Moscow cyber war'", *BBC*, 17 May 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm

[115] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

[116] Andrei Zlobin, "Who is behind the cyber war between Russia and Estonia", *Vedomosti*, 28 May 2007, http://www.vedomosti.ru/smartmoney/article/2007/05/28/3004

[117] Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack", *Wired*, 22 August 2007, http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/

[118] "Estonian DDoS - a final analysis"

[119] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", *Schneier on Security*, 7 July 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html

[120] "Estonia asks for Russian help to find Web criminals", *Reuters*, 6 June 2007, http://www.reuters.com/article/2007/06/06/us-estonia-russia-internet-idUSL0671620620070606

[121] U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008", August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[122] Jose Nazario, "Georgia DDoS Attacks – A Quick Summary of Observations", *Arbor Networks*, 12 August 2008, http://ddos.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[123] U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008".

[124] Kevin Coleman, "Cyber War 2.0 – Russia v. Georgia", *Defense Tech*, 13 August 2008, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/

[125] Gadi Evron, "Georgia Cyber Attacks From Russian Government? Not So Fast", *CSO Magazine*, 13 August 2008, http://www.csoonline.com/article/443579/georgia-cyber-attacks-from-russian-government-not-so-fast

[126] *ibid.*

[127] The full technical analysis is over a hundred pages long, but it has only been made available to the U.S. government and a number of (unnamed) cybersecurity professionals. There is, however, a nine-page summary that has been released to the public: U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008", August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[128] Jeremy Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime", *CSO Magazine*, 17 August 2009, http://www.csoonline.com/article/499778/georgia-cyberattacks-linked-to-russian-organized-crime

[129] Eneken Tikk et al, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tikk et al. 2008, p. 23).

[130] Robert McMillan, “Federal websites knocked out by online botnet attack”, *Computerworld UK*, 8 July 2009, http://www.computerworlduk.com/news/security/15588/federal-websites-knocked-out-by-online-botnet-attack/

[131] Martyn Williams, “Cyber attack hits South Korea”, *Computerworld UK*, 8 July 2009, http://www.computerworlduk.com/news/it-business/15589/cyber-attack-hits-south-korea/

[132] See also Angela Moscaritolo, “Cyber retaliation debate: Is North Korea guilty of DDoS?”, *SC Magazine*, 13 July 2009, http://www.scmagazine.com/cyber-retaliation-debate-is-north-korea-guilty-of-ddos/article/139968/

[133] *ibid.*

[134] Martyn Williams, “Was UK source of massive denial of service attack on US?”, *Computerworld UK*, 14 July 2009, http://www.computerworlduk.com/news/security/15693/was-uk-source-of-massive-denial-of-service-attack-on-us/

[135] Jeremy Kirk, “Probe into US, South Korea cyberattacks stretches around the globe”, *Computerworld UK*, 15 July 2009, http://www.computerworlduk.com/news/security/15724/probe-into-us-south-korea-cyberattacks-stretches-around-the-globe/

[136] *ibid.*

[137] Graham Cluley, “Is North Korea to blame for US cyber attacks?”, *Computerworld UK blog*, 9 July 2009, http://blogs.computerworlduk.com/computerworld-archive/2009/07/is-north-korea-to-blame-for-us-cyber-attack/index.htm

[138] The attack was dubbed “Operation Aurora” by security researchers at McAfee who discovered that the string “Aurora” was part of a file path in the malware binaries, suggesting that this was the internal name the attacker had given to the project. See George Kurtz, “Operation ’Aurora’ Hit Google, Others”, *McAfee blog*, 14 January 2010, http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others

[139] Ariana Eunjung Cha and Ellen Nakashima, “Google China cyberattack part of vast espionage campaign, experts say”, *The Washington Post*, 14 January 2014, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

For a comprehensive technical analysis of Operation Aurora, see “Protecting Your Critical Assets. Lessons Learned from Operation Aurora”, *McAfee*, March 2010, http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

[140] Google, “A new approach to China”, *Official Google Blog*, 13 January 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[141] Ariana Eunjung Cha and Ellen Nakashima, “Google China cyberattack part of vast espionage campaign, experts say”, *The Washington Post*, 14 January 2014, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

[142] Dmitri Alperovitch, McAfee’s vice president for threat research, quoted in Kim Zetter, “’Google’ Hackers Had Ability to Alter Source Code”, *Wired*, 3 March 2010, http://www.wired.com/threatlevel/2010/03/source-code-hacks/

[143] It is also widely assumed that the People's Liberation Army possesses both defensive and offensive cyber capabilities. See e.g. Brian M. Mazanec, *The Art of (Cyber) War* (Mazanec 2009).

[144] "Accusation of Chinese government's participation in cyber attack 'groundless': ministry", *Xinhua*, 25 January 2010, http://news.xinhuanet.com/english2010/china/2010-01/25/c_13149276.htm

[145] Scott Shane and Andrew W. Lehren, "Leaked Cables Offer Raw Look at U.S. Diplomacy", *The New York Times*, 28 November 2010, http://www.nytimes.com/2010/11/29/world/29cables.html?_r=1&hp

[146] Erick Schonfeld, "WikiLeaked diplomatic cables confirm China's Politburo was behind Google hacking incident", *TechCrunch*, 28 November 2010, http://techcrunch.com/2010/11/28/wikileaked-cables-china-google/

[147] Incidentally, this is true for all the diplomatic cables published by Wikileaks. They provide a unique perspective into the inner workings of US foreign policy, but should be regarded as snapshots of one individiual perspective rather than confirmed information. Unfortunately, this is usually – intentionally or unintentionally – overlooked.

[148] David A. Fulghum et al, *Cyber-Combat's First Shot* (Fulghum et al. 2007).

[149] Sally Adee, "The Hunt for the Kill Switch, *IEEE Spectrum*, May 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

[150] Thomas Rid, *Cyber War Will Not Take Place* (Rid 2012, p. 17).

Chapter 6

Case Study: Stuxnet

This chapter presents a detailed case study of Stuxnet, a sophisticated computer worm that is widely considered to be an act of cyber warfare by Israel against the Natanz nuclear enrichment facility in Iran:

> *Mossad's miracle weapon: Stuxnet opens new era of cyber war*[151]

If newspaper coverage is to be believed, Israel has declared cyber war against Iran[152] and succeeded in carrying out a significant strike against Iran's nuclear programme – not through a squadron of F16s but through a piece of computer software, a worm called Stuxnet. Is this really the case though, or are the media jumping to conclusions? The following represents an attempt to separate fact from fiction regarding the Stuxnet incident. It summarises what is actually known about the computer worm and its effects, and what is mere speculation at this point.

I will first explain the Stuxnet attack from a technical perspective in order to provide a foundation for further analysis. Then I present what is known about the target of the attack. Based on this information, I discuss who might be behind Stuxnet by asking the question of who would have the means and the motive to carry out such an attack. Finally I conclude this case study by summarising the general lessons that can be to drawn from Stuxnet.

6.1 The Technical Dimension

Stuxnet[153] is a piece of malicious computer software or *malware* discovered in June 2010. More specifically, it is a *worm* – a small program that secretly takes control over a computer and replicates itself across a network. Internet worms are common. However, Stuxnet differs from other worms in three ways: It does not spread via the Internet, it does not actually target Windows machines, and it is unusually complex and sophisticated.

Stuxnet is distributed primarily via USB sticks

Most worms spread over the Internet. They look for any kind of Internet connection and copy themselves. Stuxnet distributes itself primarily via removable drives such as USB sticks. The worm hides on a USB stick; if this device is then plugged into a computer running Windows, it will infect the computer. This scheme allows Stuxnet to infect machines that are not connected to the Internet. For security reasons, computers at industrial facilities are often disconnected from the global network – a procedure known in IT security as “air gapping” (having a physical distance – a gap filled with air – between the machine and the Internet). Air gapping secures the internal network of a facility from most malware infections. But it did not help in the case of Stuxnet. If the worm was on the USB stick of an employee of the secure facility, he or she might take the infected device to work and unwittingly infect the secure facility. Once Stuxnet is on an internal network (LAN), it also spreads across that network.

Stuxnet targets a specific industrial control system

Stuxnet infects Windows computers, but it does not actually do any damage on these computers. Its real target is an industrial control system, specifically a *Programmable Logic Controller (PLC)*. PLCs are small special-purpose computers – usually roughly the size of a toaster – that are widely used to control industrial processes in factories, refineries, power plants etc.

> The programmable logic controller, or PLC, is one of the most critical pieces of technology you’ve never heard of. They contain circuitry and software essential for modern life and control the machines that run traffic lights, assembly lines, oil and gas pipelines, not to mention water treatment facilities, electric companies and nuclear power plants.[154]

PLCs do not run Windows, but they are usually connected to regular Windows computers. In order to communicate with and program the PLC, you connect your Windows machine to the PLC and send it commands or get data from it. This is how Stuxnet works: After infecting a Windows computer, Stuxnet looks for the *Siemens SIMATIC WinC/Step7* controller software on that computer. If it does not find the Step7 software, it does nothing.[155] If it does find the Step7 software, it infects this software in order to manipulate the PLC. It intercepts commands going from the Step7 software to the PLC and replaces them with its own malicious instructions. These changes are highly specific, which indicates that Stuxnet targets a specific system.

What is that target PLC? Symantec's analysis of Stuxnet found that the worm looks for *high-frequency converter drives*, also known as *AC drives*.[156] An AC drive is a device to control the speed of a motor – the higher the output frequency, the higher the speed of the motor:

> Frequency converters modulate the speed of motors and rotors in things like high-speed drills that are used to cut metal parts in factories and in paper mills to force pulp through a grate. Increase the frequency of the drive, and the rotor increases its spin.[157]

Stuxnet searches for specific AC drives made by two manufacturers: *Vacon* (based in Finland) and *Farao Paya* (based in Iran). More concretely, the source code of Stuxnet shows that it is targeting a facility that has 33 or more of the frequency converter drives installed, all operating at high frequencies between 807Hz and 1,210Hz.[158]

If Stuxnet finds such a facility, it does the following: After an initial period where it is dormant for two weeks, Stuxnet increases the frequency of the motors to 1,410Hz for 15 minutes. Then it restores the frequency back to normal (1,064Hz) and leaves it at this level for 27 days. After 27 days, it changes the frequency down to 2Hz for 50 minutes, then restores it again to 1,064Hz and waits for another 27 days before repeating the sequence. By interfering with the speed of the motors, Stuxnet thus sabotages the normal operation of the industrial control process.[159]

This mode of operation gives some important clues about the target of Stuxnet. As Eric Chien, one of the researchers who deciphered the Stuxnet code, put it:

> Stuxnet's requirement for particular frequency converter drives and operating characteristics focuses the number of possible speculated targets to a limited set of possibilities. Stuxnet requires the frequency converter drives to be operating at very high speeds, between 807 Hz and 1210 Hz. While frequency converter drives are used in many industrial control applications, these speeds are used only in a limited number of applications.

> We are not experts in industrial control systems and do not know all the possible applications at these speeds, but for example, a conveyor belt in a retail packaging facility is unlikely to be the target. Also, efficient low-harmonic frequency converter drives that output over 600Hz are regulated for export in the United States by the Nuclear Regulatory Commission as they can be used for uranium enrichment.[160]

These high frequencies thus seem to point to a specific target. (I will explore below what that target is likely to be.)

Stuxnet is a very sophisticated piece of malware

As worms go, Stuxnet is unusually advanced: It uses five zero-day exploits, two stolen digital certificates, and it goes to great lengths to hide its presence.

1. **Stuxnet exploits four *zero-day vulnerabilities* in Windows**[161] and an additional zero-day exploit in the Step7 software. Once a vulnerability (a software problem that makes an attack possible) becomes known, it usually gets fixed quite quickly through software updates (patches). A "zero-day" is a vulnerability that has been known for zero days (i.e. not at all) when a malware exploiting it is released.

   > Zero-days are the hacking world's most potent weapons: They exploit vulnerabilities in software that are yet unknown to the software maker or antivirus vendors. They're also exceedingly rare; it takes considerable skill and persistence to find such vulnerabilities and exploit them. Out of more than 12 million pieces of malware that antivirus researchers discover each year, fewer than a dozen use a zero-day exploit.[162]

   The fact that Stuxnet uses *five* zero days is highly unusual and means that considerable resources must have been put into the development of the worm. (This point will be discussed further below.)

2. **Stuxnet uses stolen digital certificates to install its drivers.** To control the PLC, Stuxnet has to install its own driver into the Windows operating system. Drivers have to be digitally signed to ensure that they are genuine and not harmful. Windows checks these digital certificates to avoid malware from having access to critical parts of the system. To get around this, Stuxnet used two stolen

digital certificates – one from *Realtek Semiconductor Corp* and (when the theft was discovered on July 16th 2010 and the certificate was revoked) another one from *JMicron Technology Corp*. Since Stuxnet was signed with these legitimate certificates, it could install its drivers despite this protection mechanism of Windows. Getting access to these certificates was not trivial and probably required physically breaking into the premises of these two vendors.[163] Again, this is a level of determination not usually found in the malware world.

3. **Stuxnet is excellent at hiding its presence.** While manipulating the commands sent to the frequency converter drive, the worm sends back false data to the controller that make it look as if everything is working as usual:

> At the same time, another portion of Stuxnet disabled any automated alarms that might go off in the system as a result of the malicious commands. It also masked what was happening on the PLC by intercepting status reports sent from the PLC to the Step7 machine, and stripping out any sign of the malicious commands. Workers monitoring the PLC from the Step7 machine would then see only legitimate commands on the device – like a Hollywood heist film where jewellery thieves insert a looped video clip into a surveillance camera feed so that guards watching monitors see only a benign image instead of a live feed of the thieves in action.[164]

To summarise: Stuxnet is a sophisticated computer worm that spreads via USB sticks and infects Windows computers in order to sabotage a specific industrial control system. The target system uses high-frequency converter drives made by one of two manufacturers (*Vacon* in Finland and *Farao Paya* in Iran) and it operates at high frequencies (between 807 Hz and 1,210 Hz). This is the extent of what is known about Stuxnet. We do not know who wrote Stuxnet, whether it achieved its goal, or what concrete facility was its target. At this point and unless new evidence comes up, we can only speculate about these questions.

6.2 The Target

As discussed above, it is not known what the actual target of Stuxnet was. But there are a number of indications that seem to point to one specific installation: the *Natanz* fuel enrichment plant in Iran.

Focus of Stuxnet infections: Iran

Two facts support the assumption that the target was in Iran: The majority of infected computers were in Iran, and the first Stuxnet infections appeared in Iran. At the end of September 2010, there were approximately 100,000 infected computers world-wide. The majority of these – more than 60% – were in Iran, followed by Indonesia at about 18% and India at close to 10%.[165]. The researchers at Symantec analysing Stuxnet discovered that every instance of the worm contained the domain name and time stamp of all previous systems it had infected – a kind of "family tree" making it possible to trace it back to the first infected machine. They found that five organisations in Iran had been the first targets in June and July 2009, and they were hit again in March, April and May 2010.[166]

An accident at Natanz?

On July 17 2009, WikiLeaks posted the following note:

> Two weeks ago, a source associated with Iran's nuclear program confidentially told WikiLeaks of a serious, recent, nuclear accident at Natanz. Natanz is the primary location of Iran's nuclear enrichment program. WikiLeaks had reason to believe the source was credible however contact with this source was lost. WikiLeaks would not normally mention such an incident without additional confirmation, however according to Iranian media and the BBC, today the head of Iran's Atomic Energy Organization, Gholam Reza Aghazadeh, has resigned under mysterious circumstances. According to these reports, the resignation was tendered around 20 days ago.[167]

It has been impossible to independently verify whether this accident did indeed take place or to get any details about it. However, the resignation of the head of Iran's Atomic Energy Organization has been officially confirmed; no reasons were given for Aghazadeh's sudden resignation.[168] Furthermore, according to official IAEA data, there was a substantial reduction in the number of operating centrifuges in Natanz around the time of the accident Wikileaks wrote about:

> As of November 2, 2009 the number of centrifuges enriching uranium at the Natanz Fuel Enrichment Plant (FEP) has declined again, this time

> to 3,936 (the same number that were enriching in February 2009). This represents a fifteen percent decrease in the number of centrifuges enriching compared to August 12, 2009, when the IAEA last publicly tallied the number centrifuges enriching.[169]

Official Iranian sources referring to a cyber attack

There has also been official confirmation from Iran that a sophisticated computer worm infected industrial plants throughout the country. In September 2010, the semi-official Mehr news agency quoted an official from the Ministry of Industry and Mines, Mahmud Liai, as saying that 30,000 computers had been affected, and that the worm was "part of the electronic warfare against Iran.".[170]

Another high official, Reza Taghipour from the Ministry of Communications and Information Technology, referred to the attack as well. However, he downplayed the situation, saying that "the effect and damage of this spy worm in government systems [was] not serious" and that it had "more or less" halted.[171]

The first acknowledgement that the worm had hit Iran's *nuclear* facilities came from Ali Akbar Salehi, head of Iran's Atomic Energy Organization, on November 23 2010: "One year and several months ago, Westerners sent a virus to [our] country's nuclear sites", Salehi said, however asserting that the malware had been disabled without actually harming any equipment.[172]

Technical correlation between Stuxnet and Natanz

Finally, there are also indications on a technical level that an enrichment facility – rather than for instance a nuclear power plant such as Bushehr – was the target. Stuxnet works in a synchronised way, spreading its attack over many identical nodes. This is consistent with the setup of an enrichment centrifuge plant, which consists of thousands of identical units that are arranged in serial patterns called "cascades". Nuclear power plants, on the other hand, contain a wide variety of different subsystems – they are not as massively scaled in a parallel way.

The correlations between Stuxnet and Natanz go even deeper than that:

- David Albright at the Institute for Science and International Security (ISIS), which closely monitors Iran's nuclear program, has pointed out that Stuxnet targeted devices configured in groups of 164. Each of Natanz' cascades consists of exactly 164 centrifuges.[173]

- Natanz' centrifuges operate at a nominal frequency of 1,064Hz – the exact frequency that Stuxnet resets the frequency drive to after spinning it up or down.[174]
- ISIS also reported that a series of failures at Natanz in mid- to late 2009 led to 984 centrifuges being taken out of action. There is a section in the Stuxnet code that appears to sends commands to exactly 984 units that are linked together.[175]

All these indications seem to point to Natanz being the target of Stuxnet.

6.3 Who Was Behind Stuxnet?

Even before all the technical details about Stuxnet's mode of operation were known, the media was quick to conclude who was to blame:

> The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet.[176]

This was the gist of most newspaper articles on the Stuxnet incident. There is no actual proof, however, that Israel was behind Stuxnet. Of course this is one of the particularities of cyber attacks – conclusive attribution is almost never possible. At best it is possible to infer who *might* have been the attacker based on the specific features of the attack and the larger context. It is of crucial importance when making such an inference to avoid drawing the wrong conclusions. An obvious connection to one actor might be an indication that this actor was the attacker – or it might mean that *another* actor tried to *make it look as if* they were the attacker.

In a way, analysing a cyber attack is like solving any crime. The most important questions to ask are *Who had the means?* and *Who had a motive?* If you can answer these questions, you have come a long way towards finding your prime suspect. Let us thus apply these questions to the Stuxnet incident.

Who had the means?

Stuxnet was far from trivial to create. There are two factors to consider in this regard – the financial aspect and the intelligence aspect.

1. The financial aspect

Stuxnet was expensive to create – far more expensive than the usual piece of malware. Sandro Gaycken, cyber war expert and professor at the Free University Berlin, estimates that all in all, Stuxnet cost about 1.5 million USD to create.[177]

First of all, there was the manpower needed to develop the worm. Computer security expert Bruce Schneier calculates that it took eight to ten qualified developers six months to write Stuxnet.[178]. Symantec's estimates are similar: "The full cycle may have taken six months and five to ten core developers not counting numerous other individuals, such as quality assurance and management."[179] The researchers at F-Secure put the figure even higher: "We estimate that it took over 10 man-years to develop Stuxnet."[180]

Secondly, as mentioned above, Stuxnet uses four zero-day exploits in Windows – bugs in the operating system that were not known at the time that Stuxnet was released. Zero-days are difficult to find, and it is unlikely that the developer team behind the worm discovered these vulnerabilities themselves. More likely, they bought the knowledge on the black market, where criminal hacker groups sell zero-day exploits to the highest bidder. And they are expensive: "A single remote code execution zero-day in a popular version of Windows could go for anything between $50,000 to $500,000."[181]

The financial aspect means that the Stuxnet project would have been beyond the means of petty criminals. It also rules out the possibility that Stuxnet was written by some hackers in order to show off or "just for fun" – *for the lulz*, as the saying in the hacker community goes.

2. The intelligence aspect

Even more significant than the cost of writing Stuxnet is the intelligence aspect. Industrial control systems are very specific and each installation is unique. In order to create Stuxnet, the attacker needed to have in-depth inside knowledge about the target. As Ralph Langner, one of the first IT security researchers to analyse Stuxnet, pointed out:

> We know from reverse engineering the attack codes that the attackers have full, and I mean this literally, full tactical knowledge of every damn detail of this plant. So you could say in a way they know the plant better than the Iranian operator.[182]

It is not known how the attackers got this inside information. There are two possibilities – either someone who had access to the plans, schematics, and software configuration at the target side provided them to the attackers, or they used another piece of malware to infect the target and retrieve this information. The latter would be very difficult to do, since industrial facilities are usually not connected to the Internet. (This is precisely why Stuxnet spread via infected USB sticks rather than online.) Thus even if the attacker could get this malware into the plant – for instance using infected USB sticks, as with Stuxnet –, how would they get the information out? Therefore it seems most likely that the intelligence on the target was acquired in a more traditional manner. In other words, whoever wrote Stuxnet probably had a collaborator inside the target facility.

This now basically rules out organised crime as the attacker as well. While large criminal groups might have the financial resources to invest 1.5 million USD in an attack, they would not likely be in a position to get this kind of inside access. Given enough money, everything is possible of course – but as there is no obvious way to make money from Stuxnet, why would any criminal group invest this extremely high amount of resources in an operation without a payoff? This leaves one possibility – that a state actor was behind Stuxnet. This is also the consensus among researchers who have analysed the worm, including the IT security experts at F-Secure:

> Looking at the financial and R&D investment required and combining this with the fact that there's no obvious money-making mechanism within Stuxnet, that leaves only two possibilities: a terror group or a nation-state. And we don't believe any terror group would have this kind of resources.[183]

Dave Clemente, a researcher into conflict and technology at the International Security Programme at Chatham House in London, reached the same conclusion:

> You look at the Stuxnet worm. It is of such complexity it could only be a state behind it.[184]

Who had a motive?

Given the substantial resources needed to create Stuxnet, who might be the potential attackers? I will first examine the most widely believed theory – that Israel was behind Stuxnet, perhaps with the support of the U.S. – and then discuss alternative explanations that have been suggested.

1. Israel

Israel's concerns about Iran's nuclear programme are well known. Israel has also previously carried out strikes against supposed nuclear facilities in other countries in the region. In 1981, an Israeli air strike destroyed a nuclear reactor facility under construction at Osirak in Iraq.[185] In 2007, Israel bombed a suspected nuclear research complex at Al Kibar, near Deir ez-Zor in Syria.[186] Stuxnet might be the cyber equivalent to these attacks – an attempt to do something similar in Iran, albeit in a more subtle way. There are two indications that seem to point to Israel as being behind Stuxnet: indirect references to Stuxnet by Israeli and US officials, and a number of clues in the Stuxnet source code itself.

Exhibit A: Indirect references to Stuxnet by Israeli and US officials

There have been a number of references by officials from Israel and the United States that can be seen as indirectly acknowledging Stuxnet as their successful operation.

The Israeli news site *Ynet News* published an article on a potential cyberwar against the Iranian nuclear programme on July 7th 2009, around the time that Stuxnet was probably deployed. Even though the article did not reference Stuxnet (which had not been discovered at the time), in hindsight there appear to be some striking correlations. An unnamed retired Israeli security cabinet member was quoted as saying that

> We came to the conclusion that, for our purposes, a key Iranian vulnerability is in its on-line information. We have acted accordingly.[187]

The article pointed out that malicious computer software could be used to "to corrupt, commandeer or crash the controls of sensitive sites like uranium enrichment plants". Even infected USB sticks were mentioned as a way to bypass security precautions at sensitive sites:

> As Iran's nuclear assets would probably be isolated from outside computers, hackers would be unable to access them directly. Israeli agents would have to conceal the malware in software used by the Iranians or discreetly plant it on portable hardware brought in, unknowingly, by technicians. *"A contaminated USB stick would be enough,"* Borg said.[188]

The British *Daily Telegraph* reported that at a retirement party for the head of the Israel Defence Forces, Lieutenant General Gabi Ashkenazi, a video was played that showed his operational successes. This video supposedly included references to Stuxnet and a tribute from the director of Mossad at the time, Meir Dagan, thanking Ashkenazi for his contribution to disrupting the Iranian nuclear enrichment programme.[189]

When asked about Stuxnet, General Michael Hayden, former head of the NSA and director of the CIA, just said "This was a good idea, alright?"[190] Gary Samore, the Obama administrations's chief strategist for combatting weapons of mass destruction, similarly declined to comment on Stuxnet directly, then added:

> I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated.[191]

Exhibit B: Clues in the source code

There are two curious clues in Stuxnet itself that have been interpreted as connecting the worm to Israel:

1. The Stuxnet source code contains the following text string, obviously the path to where the author of Stuxnet stored the files on his or her computer: *b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb*

   "Myrtus" is another name for the myrtle plant. However, it has also been interpreted to be a reference to the Jewish queen Esther who, according to a legend from the 4th century BCE, saved Persian Jews from being massacred. Esther's name in Hebrew is *Hadassah*, which also means myrtle.[192]

2. Stuxnet sets a registry value in Windows to indicate that a computer has already been infected with the worm. This value is *19790509*, which most likely indicates a date: May 9th, 1979. Again, this has been linked to Israel: On that date, the Persian Jewish businessman Habib Elghanain was executed in Tehran after being convicted of spying for Israel.[193]

Objection!

All these clues do not necessarily prove Israel's involvement. For instance, looking at the path *b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb*: The connection to queen Esther is tenuous at best. Rather than referring to the Hebrew name Hadassah, *myrtus* is much more commonly known as the botanical term for the myrtle family of plants, which includes the guava plant. So perhaps it simply indicates that the author of Stuxnet was interested in botany. It could also mean *myRTUs* – “my RTUs” – an abbreviation for the common technical term “*R*emote *T*erminal *U*nits”, which the author of Stuxnet certainly was familiar with. As Mary Landesman pointed out, “In SCADA environments, RTU is a commonly used term for remote terminal unit. Isn’t it more plausible that the Stuxnet author named the folder myrtus (meaning My RTUs) then realized it also read myrtus, the botanical term, and hence named his file guava?”[194]

The same is true for the date 19790509. The execution of Habib Elghanain was just one of many incidents that happened on that date, and in any case it is not a well known event.

> Is it a date that the people of Israel would hold close to their hearts? Probably not. Habib may have been Jewish, but he was also an Iranian citizen – not an Israeli. It’s doubtful most people from Israel have even heard of him. On the date of his execution for alleged spying, he was put to death alongside 37 other men (most of whom were also convicted of spying). He was the only Jewish person among them.[195]

The connection to Habib only makes sense if one already assumes a link to Israel. Otherwise, it could mean anything – for all we know, it might just have been the author’s birthday.

Even assuming that these clues in the source code point to Israel, this does not necessarily indicate Israel’s involvement. The exact opposite could be the case, as security expert Bruce Schneier pointed out:

> Sure, these markers could point to Israel as the author. On the other hand, Stuxnet’s authors were uncommonly thorough about not leaving clues in their code; the markers could have been deliberately planted by someone who wanted to frame Israel. Or they could have been deliberately planted by Israel, who wanted us to think they were planted by someone who wanted to frame Israel. Once you start walking down this road, it’s impossible to know when to stop.[196]

This was also the conclusion that the researchers at Symantec came to: “Symantec cautions readers on drawing any attribution conclusions. Attackers would have the natural desire to implicate another party.”[197]

The fact that Israeli and American officials appear to have been indirectly bragging about Stuxnet does not prove anything either. Obviously any cyber warfare unit would be more than happy to be considered the masterminds behind the most complex malware in the history of information technology. Iran, on the other hand, would use any opportunity to blame its enemy Israel for problems in its nuclear programme, even if these problems had in reality been of a purely technical nature. In other words, all the references to Stuxnet may be the result of actors trying to exploit the situation after the fact. This does not necessarily mean that the same actors were involved in bringing about that situation.

If not Israel, who else could be behind Stuxnet? A number of alternative theories have been suggested:

2. China

Jeffrey Carr, author of the book *Inside Cyber Warfare*[198], proposed that China was behind Stuxnet. China has clearly stated its opposition to Iran's goal to develop nuclear weapons capabilities.[199] At the same time, Iran is China's third largest supplier of oil after Saudi Arabia and Angola, so Beijing would be reluctant to openly take steps against them. Stuxnet could have been a way for China to secretly interfere with Iran's nuclear programme.

> What better way to accomplish that goal than by covertly creating a virus that will sabotage Natanz' centrifuges in a way that simulates mechanical failure while overtly supporting the Iranian government by opposing sanctions pushed by the U.S. It's both simple and elegant. Even if the worm was discovered before it accomplished its mission, who would blame China, Iran's strongest ally, when the most obvious culprits would be Israel and the U.S.?[200]

China would have been in an excellent position to create Stuxnet:

1. Iran's centrifuges are of Chinese design, so they would have intimate knowledge of how they function.

2. The Vacon frequency converter drives targeted by Stuxnet are manufactured at the Suzhou facility in China.

3. RealTek, the company whose digital certificates were stolen in order to allow Stuxnet to install its drivers on Windows, has an office in Suzhou in China.

4. The Chinese government has direct access to the source code of the Windows operating system and has set up a lab to study it, specifically checking for security loopholes.[201] This would make it much easier for their developer team to find the four zero day vulnerabilities used in Stuxnet.

It is also interesting to note that there were no early reports of Stuxnet infections in China, even though the Siemens Step7 software is widely used in the industry there. It was only three months after Stuxnet was discovered that Chinese media suddenly reported a large number of infections. The report itself contains a noteworthy reference to the creators of Stuxnet. As Carr points out:

> That report originated with a Chinese antivirus company called Rising International, who we now know colluded with an official in Beijing's Public Security Bureau to make announcements encouraging Chinese citizens to download AV software from Rising International (RI) to fight a new virus that RI had secretly created in its own lab. Considering this new information, RI's Stuxnet announcement sounds more like a CYA strategy from the worm's originators than anything else.[202]

3. A cyberwar unit conducting a field test

Sandro Gaycken, security researcher and professor at the Free University Berlin, argues that Stuxnet was not actually targeting Iran. The focus on Iran was merely a ruse to hide its purpose, In reality, Gaycken suggests, Stuxnet was:

> a field test of a cyber weapon in different security cultures, testing their preparedness, resilience, and reactions, all highly valuable information for a cyberwar unit.[203]

According to Gaycken, Stuxnet was created and spread by a military cyber warfare unit in order to learn more about how such an operation would work in the real world. There are two indications that support this hypothesis:

First, the fact that Stuxnet infected more than 100,000 computers world-wide suggests that Iran was not the only target of the worm. A professional attacker who wanted to cause damage in Iran only would have installed the software at just one facility and avoided wider distribution. This way, the worm would most probably have remained undetected and the victim would not have been able to protect itself against it. Stuxnet could even have been used another time for another attack – which is impossible now that it is widely known.

Secondly, the Stuxnet worm attempts to "phone home" – it tries to initiate a network connection to one of two command and control servers, *www.mypremierfutbol.com* and *www.todaysfutbol.com*, hosted on servers in Malaysia and Denmark.[204] If it is able to reach one of these servers, Stuxnet reports detailed information about the infected machines, including the computer's name, internal and external IP address, its operating system and version and whether the Step7 software was installed on the machine. It can also update itself with new functionality from these servers or install more software on the infected machines. If Stuxnet was supposed to only attack Natanz in Iran, this behaviour does not make sense. The attacker would have known that the facility is not connected to the Internet, so it would not be possible for Stuxnet to reach the servers. In fact, attempting to initiate an Internet connection makes it much more likely that the worm is detected (since someone might notice the unusual network traffic). However, if Stuxnet was a global test of a new cyber "weapon", the majority of infected machines would be online – and the attackers would want to collect just this kind of information.

Cyber warfare has become a hot topic in the last few years, and there are several states which are known or suspected to have offensive cyber war capabilities, including the US, Russia, China, Japan, North Korea, Israel, France, the UK, and Germany.[205] Any one of these could have decided that it was time to test their new digital arsenal in order to get some real-life experience of the possibilities and limits of cyber operations.

4. A research project that got out of control

Stuxnet could also have been a research project that got out of control. This hypothesis is similar to the idea that Stuxnet was a field test of a new cyber weapon, except that it was not released intentionally but "escaped" by mistake.

Military or civilian researchers exploring the potential of a cyber attack on industrial infrastructure may have created Stuxnet just to test it in a contained laboratory environment. Through an accident, the worm got out and started to spread world-wide. This would be consistent with the high budget required to create Stuxnet, since such a research group would have had access to the necessary financial resources. It would also make sense that a facility like Natanz would be have been chosen as a hypothetical target to simulate in the lab.

If Stuxnet was released accidentally, this would account for the fact that the worm tries to establish a connection to a command-and-control server and upload data about the infected machine. This would be precisely the kind of functionality that researchers would want to test. An accidental "escape" would also explain Stuxnet's uncontrolled global spread.

5. Iran

Stuxnet might even have been created by Iran in order to blame Israel for trying to disrupt its "peaceful" nuclear research programme. The cyber attack on Natanz could be an attempt by the Iranian regime to bolster its internal standing by underlining the danger posed by the external arch enemy, Israel.

This would explain how the "attacker" could have had access to so much detailed inside information about a highly secure facility. It would also explain the obvious clues in the Stuxnet code implicating Israel. It is hard to imagine that any attacker smart enough to create Stuxnet would accidentally leave such references to their identity, unless they wanted these references to be found.

6. An unknown attacker with an unknown motive

If we assume that Natanz was not the actual target of Stuxnet (and again, we do not actually know that it was), it becomes impossible to say who the creators of Stuxnet were, what their motive was, and whether they achieved their goal. In addition to the hypotheses outlined above, any number of other scenarios could be the case.

For instance, Stuxnet might have been an act of **corporate sabotage to discredit Siemens**. Since the worm specifically targets Siemens' Step7 software, it may have been an attempt by a competing company to create distrust in Siemens products, especially when it comes to high-security industrial software.[206] I consider this explanation to be unlikely though, since it does not take into account that the greatest effort in creating Stuxnet was getting the specifics of the target facility's operation. A scheme to discredit Siemens would have worked just as well or better if the worm interfered with any computer running Step7, not just the ones using the two specific AC converter drives.

Stuxnet may also have been **a demonstration of cyber warfare capability**, as Bruce Schneier has suggested:

> [Stuxnet could be] a message. It's hard to speculate any further, because

> we don't know who the message is for, or its context. Presumably the intended recipient would know. Maybe it's a "look what we can do" message. Or an "if you don't listen to us, we'll do worse next time" message. Again, it's a very expensive message, but maybe one of the pieces of the message is "we have so many resources that we can burn four or five man-years of effort and four zero-day vulnerabilities just for the fun of it." If that message were for me, I'd be impressed.[207]

Or... any other explanation you can come up with. *At this point, we simply do not know.*

6.4 Conclusions

There are a number of lessons that can be drawn from the Stuxnet incident:

1. Conclusive attribution of cyber attacks is impossible.

As the analysis above has shown, it is far from certain that Stuxnet was a cyber attack by Israel against Iran. While the technical details of the worm are well understood at this point, conclusive attribution is impossible. This is unlikely to change in the future. The indications that seem to point to Israel as the attacker are all tentative, and could have been planted by another actor in order to frame Israel. It is not even clear that the Natanz facility in Iran was in fact the prime target of the worm. This uncertainty is nothing specific to Stuxnet but a general feature of cyber operations.

2. Cyber warfare is a legal grey area.

Was Stuxnet an act of (cyber) war? This is an open question. As discussed in detail in Chapter 4, whether a cyber attack qualifies as an armed attack under the UN Charter depends on the circumstances and the consequences. Since the actual effects of Stuxnet have not been confirmed, this is impossible to determine in this case. If Stuxnet did indeed cause physical damage to the Natanz facility, it might constitute an act of war. However, even in this case it would have to be conclusively established that a specific state actor was behind it – which, as we have seen, is not possible based on the information that is available.[208]

3. Industrial infrastructure can be a target of cyber attacks.

Even though we do not know who was behind Stuxnet, the worm has proven that it is possible to cause physical damage by manipulating computer software. While this has been known in theory for a long time, Stuxnet represents the first incident where such an attack has taken place in the real world, outside of a laboratory setting. There are fundamental information security issues related to industrial control systems that have not been adequately addressed, and it is to be expected that more attacks similar to Stuxnet might occur in the future.

4. Cyber crime is a main actor in state-sponsored cyber operations.

One very interesting aspect of Stuxnet is the connection between cyber crime and state action: state actors are capitalising on technology that is developed by organised criminal groups. The creators of Stuxnet did not write the worm completely from scratch. Rather, they used off-the-shelf malware components that they bought on the black market. This served two ends: First, it made the development of the worm much cheaper than it would have been otherwise. Secondly, it helped conceal who was behind Stuxnet:

> The prevalence of crime in cyberspace provides a haystack to conceal cyber espionage. [...] Stuxnet's amalgam of components helped conceal its etiology. The central challenge in attempting to identify cyber attackers underscores the dark ecology of cyberspace. Culpability is difficult to prove. Is the responsible party a Russian hacker living in New Zealand who may have contributed part of the code used for the rootkit? Or is it an intermediary that may have passed the code onto a state-based military intelligence actor? Deliberate ambiguity is an effective shield against retribution.[209]

This confluence of state actors and non-attributable third parties, especially criminal organisations, is a fundamental aspect of state-sponsored cyber operations that is likely to become even more relevant in the future.

Notes

[151] Holger Stark: “Mossad’s Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War.”, *Der Spiegel*, 8 August 2011, `http://www.spiegel.de/international/world/0,1518,778912,00.html`

[152] Michael Joseph Gross, “A Declaration of Cyber-War”, *Vanity Fair*, April 2011, `http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104`

[153] Incidentally, the name *Stuxnet* comes from a combination of file names found in the Stuxnet source code: `.stub` and `MrxNet.sys`.

[154] “Computer worm opens new era of warfare”, *CBS News*, 4 March 2012, `http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/`

[155] Absolutely nothing. Your computer could be infected with Stuxnet right now, and it would do you no harm whatsoever.

[156] Nicolas Falliere, Liam O. Murchu and Eric Chien, “W32.Stuxnet Dossier”, February 2011, `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`

[157] Kim Zetter, “How digital detectives deciphered Stuxnet, the most menacing malware in history”, *Wired*, 11 July 2011, `http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet`

[158] *ibid.*

[159] *ibid.*

[160] Eric Chien: “Stuxnet: A Breakthrough”. *Symantec Blog*, 16 November 2010, `http://www.symantec.com/connect/blogs/stuxnet-breakthrough`

[161] The exploits are: LNK (MS10-046), Print Spooler (MS10-061), Server Service (MS08-067), Privilege escalation via Keyboard layout file (MS10-073).

[162] Kim Zetter, “How digital detectives deciphered Stuxnet, the most menacing malware in history”.

[163] The two companies are unrelated, except for the fact that they both have their headquarters in the same office complex in Taiwan.

[164] Kim Zetter, “How digital detectives deciphered Stuxnet, the most menacing malware in history”.

[165] Nicolas Falliere, Liam O. Murchu and Eric Chien, “W32.Stuxnet Dossier”.

[166] Kim Zetter, “How digital detectives deciphered Stuxnet, the most menacing malware in history”.

[167] Julian Assange, “Serious nuclear accident may lay behind Iranian nuke chief’s mystery resignation”, 17 July 2009, `http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation`

[168] “Head of iran Atomic Energy Organization resigns”, *ISNA*, 16 July 2009, `http://old.isna.ir/ISNA/NewsView.aspx\?ID=News-1371331\&Lang=E`

[169] Institute for Science and International Security, "IAEA Report on Iran", 16 November 2009, http://www.isisnucleariran.org/assets/pdf/ISIS_Analysis_IAEA_Report_16Nov2009.pdf

[170] David E. Sanger, "Iran Fights Malware Attacking Computers", *New York Times*, 25.9.2010, http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html

[171] *ibid.*

[172] Kim Zetter, "How digital detectives deciphered Stuxnet, the most menacing malware in history".

[173] Kim Zetter, "Report Strengthens Suspicions That Stuxnet Sabotaged Iran's Nuclear Plant", *Wired*, 27 December 2010, http://www.wired.com/threatlevel/2010/12/isis-report-on-stuxnet/

[174] *ibid.*

[175] William J. Broad et al, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[176] Holger Stark: "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War", *Der Spiegel*, 8 August 2011, http://www.spiegel.de/international/world/0,1518,778912,00.html

[177] Interview with Prof. Gaycken, 14.3. 2012, Vienna. In my opinion, this is actually a conservative estimate and the real development cost might have been substantially higher.

[178] Bruce Schneier, "Stuxnet", 7 October 2010, http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[179] Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32.Stuxnet Dossier".

[180] F-Secure, "Stuxnet Redux: Questions and Answers", 23 November 2010, http://www.f-secure.com/weblog/archives/00002066.html

[181] F-Secure, "Stuxnet Redux: Questions and Answers".

[182] "Stuxnet: Computer worm opens new era of warfare", *CBS News*, 4 March 2012, http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/

[183] F-Secure, "Stuxnet Redux: Questions and Answers".

[184] Peter Beaumont, "Stuxnet worm heralds new era of global cyberwar", *The Guardian*, 30 September 2010, http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

[185] "1981: Israel bombs Baghdad nuclear reactor". *BBC*, 7 June 1981, http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm

[186] I discuss the cyber aspect of Operation Orchard on p. 51 *ff.* For a comprehensive report on the air strike in general, see Erich Follath and Holger Stark, "The Story of Operation Orchard: How Israel Destroyed Syria's Al Kibar Nuclear Reactor", *Der Spiegel*, 11 February 2009, http://www.spiegel.de/international/world/0,1518,658663,00.html

[187] “Wary of naked force, Israel eyes cyberwar on Iran”, *Ynet News*, 7 July 2009, http://www.ynetnews.com/articles/0,7340,L-3742960,00.html

[188] *ibid.* Scott Borg, quoted in the article, was the director of the US Cyber Consequences Unit at the time.

[189] Christopher Williams, “Israel video shows Stuxnet as one of its successes”, *The Telegraph*, 15 February 2011, http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html

[190] “Stuxnet: Computer worm opens new era of warfare”, *CBS News*, 4 March 2012, http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/

[191] William J. Broad et al, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”, *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[192] Nicolas Falliere, Liam O. Murchu and Eric Chien, “W32.Stuxnet Dossier”.

[193] “Iran: A nation still in torment”, *TIME Magazine*, 21 May 1979, http://www.time.com/time/magazine/article/0,9171,920359,00.html

[194] Mary Landesman, “Debunking the Bunk of Stuxnet”, 2 October 2010, http://antivirus.about.com/b/2010/10/02/debunking-the-bunk-of-stuxnet.htm

[195] *ibid.*

[196] Bruce Schneier, “Stuxnet”.

[197] Nicolas Falliere, Liam O. Murchu and Eric Chien, “W32.Stuxnet Dossier”.

[198] Jeffrey Carr, *Inside Cyber Warfare* (Carr 2010).

[199] “China says sanction cannot resolve Iran nuclear issue”, *Xinhua News*, 13 April 2010, http://news.xinhuanet.com/english2010/china/2010-04/13/c_13249560.htm

[200] Jeffrey Carr, “Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios”, 16 November 2010, http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf

[201] “China looks into Windows code”, *CNET News*, 29 September 2003, http://news.cnet.com/2100-1016_3-5083458.html

[202] Jeffrey Carr, “Stuxnet’s Finnish-Chinese Connection”, *Forbes*, 14 December 2010, http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

[203] Sandro Gaycken, “Wer war’s? Und wozu?”, *Die Zeit*, 26 November 2010, http://www.zeit.de/2010/48/Computerwurm-Stuxnet

[204] Robert McMillan, “Siemens: Stuxnet worm hit industrial systems”, *Computerworld*, 14.9.2010, http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems

[205] Jason Andreas and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Andreas and Winterfeld 2011).

[206] This theory was first put forward by Jeffrey Carr. See Jeffrey Carr, “Dragons, Tigers, Pearls, and Yellowcake: Four Stuxnet Targeting Scenarios”.

[207] Bruce Schneier, “Stuxnet”.

[208] For an analysis of Stuxnet as an act of war, see for instance David P. Fidler, *Was Stuxnet an act of war? Decoding a cyberattack* (Fidler 2011).

[209] James P. Farwell and Rafal Rohozinski, *Stuxnet and the future of cyber war* (Farwell and Rohozinski 2011, p. 27).

Chapter 7

Cyber Peace

As we have seen, so far no country has launched an attack that would qualify as an act of cyberwar. This will probably not change in the future. *It is unlikely that there will ever be a true cyberwar.*

7.1 Why Cyberwar Will Not Take Place

There are three main reasons why I think that cyberwar will not take place: First, serious cyber attacks are harder than it may seem. Second, cyberwar would cause collateral damage that actors may consider too great. Third, cyberwar would likely lead to an escalation into regular armed conflict. These ideas will be discussed in detail below.

I do not mean to imply that future conflicts between states may not have a cyberspace component. It is highly probable that they will. However, that component will be just a part of military operations, not the entire (nor the deciding part of the) war. Thus these wars will not be "cyberwars", but merely wars that utilise information technology in combination with other technologies.

7.1.1 Difficulty of Attacks

Serious cyber attacks are harder to accomplish than is often assumed. Let us set aside comparatively trivial attacks such as DDoS and website defacements – which, as we have seen, do not cause any serious damage and thus do not qualify as acts of (cyber) war – and consider the subset of cyber attacks that could actually cause real-world damage. Attacks on SCADA systems (see p. 19 *ff.* for a technical explanation) are the prime example for this.

SCADA attacks are usually the central element in cyberwar nightmare scenarios. For instance, a 2009 front page *Wall Street Journal* story claimed that Chinese and Russian hackers had penetrated the U.S. power grid and installed "logic bombs" at critical places in the infrastructure. These backdoors could be activated at any point, causing massive blackouts across the nation.[210] However, such stories seem to be based on imagination more than on fact. The only sources for the article's claim that digital armageddon was just one mouse-click away were "anonymous U.S. intelligence officials", which makes it hard to verify whether there is any truth to these claims.

In a speech delivered in April 2011 at the University of Rhode Island, General Keith Alexander, head of the U.S. Cyber Command, invoked the SCADA threat as well: "What I'm concerned about are destructive attacks – those that are coming." Alexander illustrated the danger of SCADA attacks by recounting an accident that had taken place at Russia's Sayano-Shushenskaya hydroelectric plant in August 2009: A turbine was ripped out of place by a sudden surge in water pressure, killing seventy-five people and causing $1.3 billion in damage. The accident happened because the bolts keeping the turbine in place had been worn down, and a sensor that was supposed to detect this had malfunctioned.[211]

Alexander presented this incident as an example of the cyber threat, implying that it would be possible to cause such a catastrophe by remotely manipulating the sensor that had failed. However, he failed to mention two key issues. First, the general safety and security standards at the power plant were notoriously poor. If the turbines had been properly maintained, the worn-out bolts would have been detected and replaced, with or without the electronic sensor. Secondly, the chain of events leading up to the accident was highly unique and unexpected. There was a fire at another power station, Bratsk, about 500 miles away. That power station had to be partially shut down, creating a drop in energy supply that the authorities sought to compensate for by increasing the output from Sayano-Shushenskaya. The sudden and unexpected spike in demand led to the failure of the turbine. Human error in estimating the capacity of the plant may well have played a significant role here.

Re-creating such a chain of events would be very hard, if not impossible, to do. As Thomas Rid observed,

> If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an acci-

> dent at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath.[212]

That is not to say that insecure SCADA systems do not pose a significant risk. They do, and this threat has to be addressed. However, the danger of "cybergeddon" has been massively overhyped, and pulling off a significant attack against a SCADA system is likely to be much more difficult than most people – including General Alexander – seem to believe.

7.1.2 Risk of Collateral Damage

Another reason why cyberwar is unlikely is that potential state actors would have much to lose – and comparatively little to win – by starting a cyberwar. Due to the interconnected nature of the global Internet, and, perhaps more importantly, the global economy, many of the systems that an aggressive cyberattack could damage are also valuable to the potential attacker. To quote James Lewis, senior fellow and director of technology and public policy at the Center for Strategic and International Studies in Washington, D.C.:

> The countries that are capable of doing this don't have a reason to. Chinese officials have said to me, "Why would we bring down Wall Street when we own so much of it?" They like money almost as much as we do.[213]

7.1.3 Risk of Escalation

The final, and perhaps most important, reason why cyberwar is less attractive than it may seem is that a cyberwar would likely escalate into a regular kinetic conflict. As mentioned earlier, the United States Department of Defense has made it clear that they reserve the right to respond to "significant cyber attacks directed against the U.S. economy, government or military" by using "all necessary means", including "kinetic capabilities".[214]

The likelihood of an escalation to kinetic warfare is correlated with the dependence of the attacked country on information technology. The higher developed the country, the higher its vulnerability to cyber attacks – and the higher the incentive to escalate. Bruce Schneier explains this using the hypothetical example of a cyberwar between the United States and North Korea:

> A country like the United States, which is heavily dependent on the Internet and information technology, is much more vulnerable to cyber-attacks than a less-developed country like North Korea. This means that a country like North Korea would benefit from a cyberwar exchange: they'd inflict far more damage than they'd incur. This also means that, in this hypothetical cyberwar, there would be pressure on the U.S. to move the war to another theater: air and ground, for example.[215]

Cyberwar is thus no subtle *alternative* to traditional war – rather it would likely just be the *prelude* to it.

This potential of escalation means that the considerations for starting a cyberwar are the same as for starting any other kind of war. Any of the countries capable of large-scale cyberwar (which includes the United States, Russia, China, Israel, and the United Kingdom) would be cautious to take that step. As James Lewis pointed out:

> The half-dozen countries that have cyber capability are deterred from cyberwar because of the fear of the American response. Nobody wants this to spiral out of control.[216]

The same is true for the U.S. considering to conduct cyberwar against an adversary, which might precipitate an escalation and (non-cyber) response from that country or one of its allies. In other words, the old balance of terror still holds, even in cyberspace.

7.2 Stopping the Militarisation of Cyberspace

Cyberwar is not likely to happen in the near future. However, there are serious cyber threats that need to be addressed, in particular the proliferation of cybercrime. My argument showing that the danger of cyberwar is overhyped should not be misunderstood to mean that all is well, and we should not worry. Quite the contrary. But framing the discussion in terms of military terms does little to address the real threats. In this, I agree with White House cyber-security coordinator Howard Schmidt, who called cyberwar *a terrible metaphor and a terrible concept*.[217]

In a 2011 working paper, technology policy experts Jerry Brito and Tate Watkins warned that the alarmist "cyberwar" rhetoric is facilitating the rise of a "cyber-industrial complex":

> Threat inflation related to cybersecurity may lead the American people and their representatives to accept unjustified regulation of the Internet and increased federal spending on cybersecurity. Since WWII, a military-industrial complex has emerged that encourages superfluous defense spending and, at times, places special interests before the public interest. We may similarly be seeing the creation of a cyber-industrial complex.[218]

Ronald Deibert, Director of the Citizen Lab, an interdisciplinary research institute focusing on global security and new technologies, also exposes the dangers of the militarisation of cyberspace, which he says will inevitably lead to the creation of a "cyber military-industrial complex". Deibert lays out that this emerging power structure can become a far larger threat than foreign military cyber operations, posing both immediate threats to the maintenance of online freedom and longer-term threats to the integrity of global communications networks.[219]

Of course, we have to be wary not to counter the cyberwar hype with a similarly exaggerated cyber-military-industrial-complex hype. But I do think it is important how we frame our approach to cyber security. As Bruce Schneier, one of the world's most renowned information security experts, points out:

> We surely need to improve our cybersecurity. But words have meaning, and metaphors matter. [...] If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of "war", we feed our fears. We reinforce the notion that we're helpless – what person or organization can defend itself in a war? – and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime.
>
> If, on the other hand, we use the more measured language of cybercrime, we change the debate. Crime fighting requires both resolve and resources, but it's done within the context of normal life. We willingly give our police extraordinary powers of investigation and arrest, but we temper these powers with a judicial system and legal protections for citizens.

> We need to be prepared for war, and a Cyber Command is just as vital as an Army or a Strategic Air Command. [...] But we're not fighting a cyberwar now, and the risks of a cyberwar are no greater than the risks of a ground invasion. *We need peacetime cyber-security, administered within the myriad structure of public and private security institutions we already have.*[220]

This *peacetime cyber-security* is what we should focus our efforts on. A few suggestions for how to approach this will be laid out in the next chapter.

Notes

[210] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies", *Wall Street Journal*, 8 April 2009, `http://online.wsj.com/article/SB123914805204099085.html`

[211] Thomas Rid, "Think Again: Cyberwar", *Foreign Policy*, March/April 2012, `http://www.foreignpolicy.com/articles/2012/02/27/cyberwar`

[212] *ibid.*

[213] James Lewis, quoted in Stuart Fox, "Why Cyberwar Is Unlikely", *Security News Daily*, 2 July 2011, `http://www.securitynewsdaily.com/830-cyberwar-unlikely-deterrence-cyber-war.html`

[214] U.S. Department of Defense, "Cyberspace Policy Report", report to Congress pursuant to the National Defense Authorization Act for fiscal year 2011, section 934, November 2011, `http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf`

[215] Bruce Schneier, "Book Review: Cyber War", *Schneier on Security*, 21 December 2010, `http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html`

[216] James Lewis, quoted in Stuart Fox, "Why Cyberwar Is Unlikely".

[217] Howard Schmidt, quoted in Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar'", *Wired*, 4 March 2010, `http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/`

[218] Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* (Brito and Watkins 2011, p. 19).

[219] Ronald Deibert, *Tracking the emerging arms race in cyberspace* (Deibert 2011).

[220] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", *Schneier on Security*, 7 July 2010, `http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html` (Emphasis added.)

Chapter 8

Recommendations

8.1 What Is To Be Done?

What can be done to address the serious cyber threats that we are facing? The following is a list of recommendations that may be useful steps to take in order to improve the situation.

Encourage public debate

One of the most important steps is to encourage a wider public debate of the issue. What is needed is a realistic discussion of the threats and risks, and how to best deal with them. This debate needs to involve not only specialists from the fields of information security and high-level policy makers but citizens in general. The policy choices that will be made in response to the cyber threats will concern everyone, and therefore the issue has to be regarded in a larger context.

In this debate, it is crucial to keep a level-headed perspective. In the words of technology policy experts Jerry Brito and Tate Watkins:

> Stop the apocalyptic rhetoric. The alarmist scenarios dominating policy discourse may be good for the cybersecurity-industrial complex, but they aren't doing real security any favors.[221]

Precisely because cyber threats are often treated as a military or national security issue, the matter tends to be shrouded in secrecy. This is problematic for a number of reasons, transparency of policy-making being just one of them. It is also counterproductive from a practical standpoint. Since most of the Internet infrastructure is privately owned, a large share of improving its security will fall to the business sector. Businesses, however, respond to market demands – and the market will only demand increased security if people are aware of the problem:

> If we put [intelligence agencies] in charge of cyber security, by their clearly secretive nature, they won't be able to put public pressure on businesses to make necessary reforms and improvements to their products. That's not where public pressure comes from.[222]

It is also important to stop conflating the various cyber threats. As I have tried to show, cyber attacks may be committed by a number of different actors for different motives. The various threats cannot be adequately addressed unless this is taken into account.

Susan Landau recently raised this point when commenting on the four cybersecurity bills (Lieberman-Collins, McCain, CISPA, and Lungren) that were under discussion in the U.S. Senate at the time of this writing:

> The point to keep in mind is that cybersecurity is not one problem but multiple ones. Protecting the control systems of the power grid from intrusion is fundamentally different from protecting private-sector proprietary information against electronic espionage, and the right set of laws, regulations, and techniques to do each properly will vary considerably. Instead of the four Congressional bills that can't agree on which way to pull, we should be devising narrowly targeted solutions that handle the different cyber risks differently. In the long run, only such targeted cybersecurity solutions are likely to be effective.[223]

Fight cybercrime

Cybercrime is behind the vast majority of cyber attacks today, and it is a growing business. Therefore, cybercrime – not cyberwar – is the main issue that we should be concerned about.

An important aspect of this is to improve international co-operation when it comes to fighting cybercrime. One part of this might be to encourage the widespread ratification and actual implementation of the Budapest Convention on Cybercrime and other relevant international treaties. Another part is to strengthen international cross-border law enforcement.

All this will only work if there is international agreement to do so, though. The main reason why cybercrime is so effective today is that there are countries that provide "safe havens" from which cyber criminals can operate. As James A. Lewis, Director of Technology and Public Policy at the Center for Strategic and International Studies, clarifies,

> Cybercriminals operate in a political context. The most skilful non-state actors live in "sanctuaries," where they are tolerated by the government. An informal arrangement between government and cybercriminal, where a cybercriminal limits criminal activity to targets outside the host nation, perhaps pays the occasional bribe to local law enforcement, and agrees to be responsive to requests for assistance in attacking targets designated by the government, would please everyone. [...]
>
> We should not forget that many of the countries that are havens for cybercrime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept. A hacker who turned his sights from Tallinn to the Kremlin would have only hours before his service were cut off, his door was smashed down and his computer confiscated.[224]

Establish confidence-building measures to avoid escalation

As explained in the preceding chapter, one of the risks of using cyber attacks as a means of warfare is that escalation is likely. Internationally agreed norms on the use of cyber "weapons" could go far towards mitigating this risk.

An international cyberwar treaty is a probably long way off – and an arms control treaty that bans or restricts the development of "cyber weapons" would be both unenforceable and might even harm cyber security.[225] But steps should be taken to move towards better understanding and cooperation. Confidence-building measures between states will greatly reduce the risk of conflict in cyberspace, especially the risk of escalation to a kinetic conflict.

A good start would be to establish a hotline between cyber commands, similar to the hotlines between nuclear commands. Note that I am not saying that the cyber threat is comparable to the nuclear threat. But having a line for high-level communication to avoid misunderstanding and over-reaction could prove essential when it comes to cyber attacks – especially due to the difficulty of attribution.

The United States and Russia are currently in the process of setting up such a hotline. The agreement seeks to improve communication and transparency in order to "reduce the chances [that] a misunderstood incident could negatively affect our relationship", as White House spokeswoman Caitlin Hayden said.[226]

Improve general IT security

This may sound obvious, but the single most important step to prevent cyber attacks is to improve the general level of IT security.

First and foremost, this means education in the general public. Most common cyber incidents could be prevented by following simple best practices, such installing anti-virus software and updating it regularly. The GCHQ has estimated that more than 80% of currently successful attacks could be defeated by following basic "cyber hygiene".[227]

It also means investing more in the security of critical systems. This includes military and government networks, which still tend to be all too vulnerable even to fairly unsophisticated attacks. To stay with the example of the UK: just recently it was reported that hackers had managed to gain access to some of the top secret systems within the Ministry of Defence, prompting Major General Jonathan Shaw, the UK military's head of cyber-security, to comment with unusual candidness:

> I think it was a surprise to people quite how vulnerable we are.[228]

Introduce smart regulations

This is probably going to be the most controversial of the recommendations I am making, but I think it is an essential component of a comprehensive cyber security strategy.

In his 2010 book *Cyber War. The Next Threat to National Security and What to Do About It*, Richard Clarke introduced the concept of the *"Defensive Triad"* – critical systems that are essential to defend. This triad consists of military networks, the high-level ISPs, and the national power grid.[229] While I disagree with much of Clarke's rhetoric in his book, I fully agree with him on this priority.

A key point here is that two parts of this triad – the high-level ISPs and the power grid – are at least partially privately owned in much of the Western world. As Bruce Schneier observed in his review of Clarke's book,

> [The high-level ISPs and the power grid] are simply too central to our nation, and too vulnerable, to be left insecure. And their value is far greater to the nation than it is to the corporations that own it, which means the market will not naturally secure it. I agree with the authors that regulation is necessary.[230]

Regulation has become something of a dirty word, invoking the spectre of needless bureaucracy stifling innovation and prosperity. However, in the case of market failures, regulation is appropriate and necessary. Corporate-owned infrastructure which has become a critical asset may be such a case.

Focus on resilience

This is a more technical point. One of the best responses to many cyber attacks is resilience.[231] This is certainly true for dealing with DDoS, but it applies in many other cases as well. Defence is important, but realistically we have to acknowledge that it will never be possible to prevent all attacks. Resilience means planning for failure – having a system in place for how to minimise the damages from an attack, and how to recover from it later:

> [Government and private companies] should ensure systems are resilient, so that if one critical computer system falls over there are backups that can take their place, and that the organisations have plans in place when things go wrong, to fix them, so the services aren't out of action for any significant amount of time.[232]

Mitigate the risk of backdoors

A threat that is often overlooked is that hardware and software may contain intentional flaws and hidden backdoors. Former U.S. Deputy Secretary of Defense William J. Lynn III was correct in identifying this as a major cause for concern:

> Computer networks themselves are not the only vulnerability. Software and hardware are at risk of being tampered with even before they are linked together in an operational system. Rogue code, including so-called logic bombs, which cause sudden malfunctions, can be inserted into software as it is being developed. As for hardware, remotely operated "kill switches" and hidden "backdoors" can be written into the computer chips used by the military, allowing outside actors to manipulate the systems from afar. The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat. Tampering is almost impossible to detect and even harder to eradicate. Already, counterfeit hardware has been detected in systems that the Defense Department has procured.[233]

To mitigate these risks, two approaches may be useful. One is to establish a secure, domestic supply chain for critical components. The second is to avoid proprietary hardware and software in favour of open-source alternatives.

Secure the supply chain for critical systems

The problem of so-called "logic bombs" (to stay with the military terminology for the moment) is of particular concern for Western states since the supply chains have become so internationalised. The majority of the computer chips used in critical systems are likely to be manufactured in the very countries that would be potential opponents in a future conflict.

The Pentagon is trying to address this issue through its *Trusted Foundry Progam*, which certifies components produced by domestic microelectronics manufacturers. The Trusted Foundry Program is a joint initiative by the U.S. Department of Defense and the National Security Agency, started in 2004 with the goal to "ensure that mission-critical national defense systems have access to leading-edge integrated circuits from secure, domestic sources".[234]

Prefer open source over proprietary alternatives

Establishing a secure domestic suppply chain may be a useful idea for increasing the security of military networks, but obviously on a larger scale rolling back globalisation and using only domestically-produced components cannot be the solution.

My suggestion for lowering the risk of backdoors and intentional errors is to use open-source software and hardware wherever possible. Detecting malicious code and finding backdoors in chips is technically impossible to do if these are proprietary products, meaning that their design is not available. With open source, the "blueprint" for all the components is open to public scrutiny. The source code, development toolchain, schematics, and plans can all be inspected and analysed to look for hidden traps. It is still a difficult task to do so, but it becomes *possible* – a mere matter of the amount of resources you are willing to spend, which will vary with the threat assessment of the system you are trying to secure.

Discussing the merits of open source would go beyond the scope of this work, so I will not go into further details here. Let me just address one argument that some readers of this thesis will certainly raise – the claim that open source is somehow less secure because it gives potential attackers the advantage of knowing more about the system they are targeting. Wouldn't it be better to keep the inner workings of any technical system hidden? The short answer is – *no*. The idea of trying to achieve better security by hiding implementation details is referred to in the information security community as *security through obscurity* – a pejorative expression, since it simply does not work. This basic rule is known as *Kerckhoffs' principle* and was first postulated in 1883 by the Dutch cryptographer Auguste Kerckhoffs in his seminal work *La Cryptographie Militaire*: "[The system] must not be required to be secret, and must be able to fall into the hands of the enemy without inconvenience."[235] Kerckhoffs was referring specifically to military cryptography, but his principle has become a fundamental and essentially uncontested tenet of the information security community. Open systems are more secure than closed ones, since they can be analysed and studied in depth. This means that any hidden flaws are likely to be discovered and fixed, whereas the problems in proprietary, closed systems remain unknown – until an attacker finds and exploits them.[236]

Let us not trade freedom for security

My final recommendation is to be wary of the fallacy that there is somehow a trade-off between security and freedom. There isn't. Security, and that includes cyber security, need not come at the expense of civil liberties. As a society and as individual citizens, we have to make sure that any attempts to make cyberspace more secure do not end up limiting our freedom of expression, privacy, and other fundamental rights.

There are currently a number of worrisome trends in Europe and the United States moving in just that direction though. One example is the *Cyber Intelligence Sharing and Protection Act* (CISPA) that is currently under consideration in the U.S. Senate. (It was already passed in the House of Representatives on 26 April 2012.[237]) The stated purpose of the bill is to allow companies and the federal government to share information to prevent or defend from cyber attacks. However, the bill is written so broadly that it would allow companies to hand over personal information to government agencies without any judicial oversight, effectively bypassing all existing privacy laws.[238] Even the White House released a statement criticising CISPA, underlining that any cybersecurity bill with information sharing provisions "must include robust safeguards to preserve the privacy and civil liberties of our citizens" and declaring that they would not support "legislation that would sacrifice the privacy of our citizens in the name of security".[239]

It will be up to us as empowered and informed citizens to oppose such legislation.

Notes

[221] Jerry Brito and Tate Watkins, "Cyberwar Is the New Yellowcake", *Wired*, 14 Feburary 2012, http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/

[222] Thomas Rid, quoted in Anna Leach, "The cyber-weapons paradox: 'They're not that dangerous'", *The Register*, 24 February 2012, http://www.theregister.co.uk/2012/02/24/cyber_weapons/

[223] Jack Goldsmith, "Susan Landau on Cybersecurity Bills", *Lawfare*, 3 May 2012, http://www.lawfareblog.com/2012/05/susan-landau-on-cybersecurity-bills/

[224] James A. Lewis, *The Korean Cyber Attacks and Their Implications for Cyber Conflict* (Lewis 2009, p. 8).

[225] Martin Libicki, "Setting international norms on cyberwar might beat a treaty", *US News Debate Club*, 8 June 2012, http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty

For a general discussion of the challenges in establishing an international cyber treaty, see e.g. Kenneth Geers, *Strategic Cyber Security* (Geers 2011, pp. 123–131) and Tom Gjelten, "Shadow Wars: Debating Cyber Disarmament", *World Affairs*, November/December 2010, http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament

[226] Ellen Nakashima, "In U.S.-Russia deal, nuclear communication system may be used for cybersecurity", *The Washington Post*, 26 August 2012, http://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html

[227] UK Cabinet Office, "The UK Cyber Security Strategy", November 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

[228] Nick Hopkins, “Hackers have breached top secret MoD systems, cyber-security chief admits”, *The Guardian*, 3 May 2012, http://www.guardian.co.uk/technology/2012/may/03/hackers-breached-secret-mod-systems

[229] Richard A. Clarke, “Cyber War. The Next Threat to National Security and What to Do About It” (Clarke 2010).

[230] Bruce Schneier, “Book Review: Cyber War”, *Schneier on Security*, 21 December 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html

[231] For a general introduction to resilience as an essential feature of a secure system, see Bruce Schneier, *Beyond Fear* (Schneier 2003, pp. 119–132).

[232] Dr. Ian Brown, interviewed by Nicole Kobie, “Q&Q: Threat of cyberwar is ’over-hyped”’, *PC Pro*, 17 January 2011, http://www.pcpro.co.uk/news/interviews/364435/q-a-threat-of-cyberwar-is-over-hyped

[233] William J. Lynn III, “Defending a New Domain. The Pentagon’s Cyberstrategy” (Lynn III 2010). Article also available online at the U.S. Department of Defense website, http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx

[234] Trusted Foundry Program, http://www.trustedfoundryprogram.org/

[235] *“Il faut que [le système] n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi”* (Kerckhoffs 1883, p. 12).

[236] For more on the general principles of systems security, see e.g. (Schneier 1996).

[237] Office of the Clerk of the U.S. House of Representatives, “Final Vote Results For Roll Call 192”, 26 April 2012, http://clerk.house.gov/evs/2012/roll192.xml

[238] Trevor Timm, “Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It”, *EFF*, 15 April 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it

[239] Brendan Sasso, “Administration pushes against bipartisan House cybersecurity legislation”, 17 April 2012, http://thehill.com/blogs/hillicon-valley/technology/222143-white-house-criticizes-cybersecurity-bill-cispa

Chapter 9

Conclusions

As this thesis has attempted to show, cyberwar is an ill-suited concept for addressing the real cyber security threats we are facing. The majority of cyber attacks that we have seen do not qualify as acts of war. Why then should we deal with them using a military framework? A military response is unlikely to solve any of the actual problems. What is needed is a *civilian* approach.

I am not saying that the threat is not real. It is. There is a large spectrum of actors abusing the Internet for their nefarious purposes. Transnational organised criminal groups have discovered that the Internet makes an excellent tool for their activities, and cybercrime has become a booming business. Fraud, extortion, identity theft, and corporate espionage are just some of the crimes that have become much easier in a globally networked world. And organised crime is not the only threat. The actions of individuals may also pose a significant risk, ranging from attempts to break into computer systems "just for fun" to politically motivated acts of online vandalism or public protest. Some – but not all – of these actions are of a criminal nature. Even potential future acts of cyber terrorism cannot be excluded.

All of these threats are serious, but we already have a system in place for dealing with them: the regular framework of law enforcement. There is no reason why criminal acts committed online should not be prosecuted using the same set of rules that would also apply offline. The legal framework will certainly need to be adapted, and deciding how exactly to deal with some of these new threats will require a prolonged and complex public debate. (For instance, is taking part in a DDoS attack to be regarded as a criminal act or as a legitimate expression of civil disobedience akin to participating in a sit-in?[240])

However, having such debates, and eventually deciding on what new legal rules we need in order to address a changed reality, is part of the healthy functioning of peacetime society. There is no reason why we should abandon this process and invoke the rules of war. The framework of law enforcement is generally successful in dealing with fraud, theft, vandalism, and acts of violence offline. It will work just as well in dealing with these issues online.

Let me underline again that I am not trying to downplay the seriousness of the threat, or to suggest that state actors do not have an interest in using cyber attacks. (They do.) But the appropriate response to these threats does not focus on (military) cyber defence but on improving civilian cyber security.[241] A continued militarisation of our approach to dealing with cyber threats will do little to address the real problems, and create a whole range of new problems instead. As Bruce Schneier pointed out, "It's about who is in charge of cyber security, and how much control the government will exert over civilian networks".[242] By framing the debate in terms of cyberwar, we are essentially accepting the idea that the open Internet has failed.

One of the consequences of being in a state of (cyber) war is that we have to accept a limitation of civil liberties.[243] There are currently a number of initiatives leading in just that direction, such as the *Cyber Intelligence Sharing and Protection Act* (CISPA) currently under consideration in the US.[244] CISPA expressly authorises the monitoring of private communications and would allow companies to hand over personal information to the government with no judicial oversight. As security researcher Jacob Appelbaum warns,

> It's not only that this data is being collected, but now they want to share it with the DHS, with the FBI, and the NSA – essentially legalizing military surveillance over U.S. citizens and the whole planet. [...] This is an existential threat to anonymity online, to privacy, and to the security of everyday people.[245]

In the end, the greatest threat to the Internet as an open platform for the free exchange of ideas, collaboration, and sharing may not come from the hackers of China's "Blue Army"[246] or even from the booming cybercrime world. It may come from those who claim they need more control over the Internet in order to "defend" it.

As I am writing these final observations, cyberwar is in the headlines once again. A recent *New York Times* article presented a detailed exposé of an alleged high-level U.S. programme to develop and use cyber attacks, code-named *Olympic Games*.[247] The *Flame* malware kit discovered at the end of May is believed to be "part of a well-coordinated, ongoing, state-run cyberespionage operation".[248] In an unexpected disclosure last week, the German government revealed that they possess offensive cyberwarfare capacities.[249]

It is a troubling picture that emerges. I have outlined why I think that cyberwar is unlikely – in particular due to the high risk of escalation to a kinetic conflict. However, I may be wrong. Certainly there is a large number of states investing heavily into the development of military cyber capabilities. And once a weapon is there, there is a temptation to use it. My call for cyber peace is also to be understood in that sense – though I realise it may already be too late.

I keep thinking of that wonderful 1983 movie *WarGames*, from which the title of this thesis is drawn. In this movie, a young man gets access to a high-level US military computer system. He thinks he is just playing a game, but in reality he is talking to a top-secret intelligent super-computer that is simulating World War Three – and is now getting ready to launch nuclear missiles against the Soviet Union. When the young man realises that he is about to cause global thermonuclear war, he wants to stop the "game", but this is no longer possible. The catastrophe is only averted when the artificial intelligence finally realises – literally in the last moment before plunging the world into nuclear annihilation – that there is only one lesson to be learnt from war:[250]

A strange game. The only winning move is not to play.

Notes

[240] In fact, this debate has already started. For an introduction to the main arguments on both sides, see e.g. Jose Nazario, *Politically Motivated Denial of Service Attacks* (Nazario 2009) and Nancy Scola, "Ten Ways to Think About DDoS Attacks and 'Legitimate Civil Disobedience' ", *TechPresident blog*, 13 December 2010, http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacks-and-legitimate-civil-disobedience

[241] To be clear, this is not about defending military systems. Of course it is important to defend military systems against cyber attacks. But that is only a small part of the picture. The question is not whether the military should take a military approach to securing its own systems. The question is whether this approach should be applied to civilian systems as well.

[242] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", *Schneier on Security*, 7 July 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html

[243] On the erosion of civil liberties during times of war, see e.g. Louis Fisher, "Civil Liberties in Time of War", *Congressional Research Service*, 7 February 2003, http://www.clas.ufl.edu/users/

rconley/conferencepapers/Fisher.pdf

[244] Trevor Timm, “Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It”, *EFF*, 15 April 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it

[245] Jacob Appelbaum interviewed on *Democracy Now!*, 26 April 2012, http://www.democracynow.org/2012/4/26/targeted_hacker_jacob_appelbaum_on_cispa

[246] China’s cyber warfare unit. See “PLA establishes ’Online Blue Army’ to protect network security”, *People’s Daily Online*, 26 May 2011, http://english.peopledaily.com.cn/90001/90776/90786/7392182.html

[247] David E. Sanger, “Obama order sped up wave of cyberattacks against Iran”, *The New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[248] Kim Zetter, “Meet ’Flame,’ the massive spy malware infiltrating Iranian computers”, *Wired*, 28 May 2012, http://www.wired.com/threatlevel/2012/05/flame/

[249] Michael Fischer, Joerg Blank and Christoph Dernbach, “Germany confirms existence of operational cyberwarfare unit”, *Deutsche Presse-Agentur*, 5 June 2012, http://www.stripes.com/news/germany-confirms-existence-of-operational-cyberwarfare-unit-1.179655

[250] “WarGames (1983) – Memorable Quotes”, *The Internet Movie Database*, http://www.imdb.com/title/tt0086567/quotes

Bibliography

Andreas, J. and S. Winterfeld (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham: Syngress.

Arquilla, J. and D. Ronfeldt (1997). *Looking Ahead: Preparing for Information Age Conflict*. Santa Monica, CA: RAND.

Brenner, S. W. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press.

Brenner, S. W. and L. L. Clarke (2010). Civilians in cyberwarfare: Conscripts. *Vanderbilt Journal of Transnational Law 43*.

Brito, J. and T. Watkins (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Working Paper No. 11-24, Mercatus Center, George Mason University. `http://mercatus.org/sites/default/files/publication/WP1124_Loving_cyber_bomb.pdf`.

Carr, J. (2010). *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media.

Clarke, R. A. (2010). *Cyber War. The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

Deibert, R. (2011). Tracking the emerging arms race in cyberspace. *Bulletin of the Atomic Scientists 67*(1), 1–8.

Dinstein, Y. (2005). *War, Aggression and Self-Defence* (4th ed.). Cambridge, UK: Cambridge University Press.

Dunlap Jr., C. J. (2011). Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly Spring 2011*, 81–99.

Farwell, J. P. and R. Rohozinski (2011). Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy 53*(1), 23–40.

Fidler, D. (2011). Was Stuxnet an act of war? Decoding a cyberattack. *IEEE Security & Privacy 9*(4), 56–59.

Fulghum, D. A., R. Wall, and A. Butler (2007). Cyber-combat's first shot. *Aviation Week & Space Technology 167*(28r–31).

Geers, K. (2011). *Strategic Cyber Security*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Hayden, M. V. (2011). The future of things cyber. *Strategic Studies Quarterly 5*(1), 3–7.

Huntley, T. C. (2010). Controlling the use of force in cyberspace: The application of the Law of Armed Conflict during a time of fundamental change in the nature of warfare. *Naval Law Review 60*, 1–40.

Jinks, D. (2003). State responsibility for the acts of private armed groups. *Chicago Journal of International Law 4*, 83–95.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires IX*, 5–83.

Kostine, S. and E. Raynaud (2009). *Adieu Farewell*. Paris: Laffont.

Kulesza, J. (2009). State responsibility for cyberattacks on international peace and security. In *Polish Yearbook of International Law*. Warsaw, Poland: Polish Academy of Sciences.

Lachov, I. (2009). Cyber Terrorism: Menace or Myth. In F. D. Kramer, S. H. Starr, and L. K. Wentz (Eds.), *Cyberpower and National Security*, pp. 437–446. Dulles, Virginia: Potomac Books.

Leverett, E. P. (2011). Quantitatively Assessing and Visualising Industrial System Attack Surfaces. Master's thesis, Darwin College, University of Cambridge.

Lewis, J. 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`.

Lynn III, W. J. (2010). Defending a new domain. The Pentagon's cyberstrategy. *Foreign Affairs September/October 2010*.

Mazanec, B. M. (2009). The Art of (Cyber) War. *Journal of International Security Affairs Spring 2009*(16).

Nazario, J. (2009). Politically motivated Denial of Service Attacks. In *The Virtual Battlefield: Perspectives on Cyber Warfare*. Lansdale, PA: IOS Press.

Reed, T. C. (2004). *At the Abyss: An Insider's History of the Cold War*. New York: Presidio Press.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies 35*(1), 5–32.

Rid, T. and P. McBurney (2012). Cyber-weapons. *RUSI Journal 157*(1), 6–13.

Schmitt, M. N. (2010). Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, pp. 151–178. National Academies Press.

Schneier, B. (1996). *Applied Cryptography*. New Jersey: John Wiley & Sons.

Schneier, B. (2003). *Beyond Fear*. New York: Springer.

Slay, J. and M. Miller (2007). Lessons learned from the Maroochy water breach. In E. Goetz and S. Shenoi (Eds.), *Critical Infrastructure Protection*, pp. 73–82. Boston: Springer.

Sommer, P. and I. Brown (2011). Reducing systemic cybersecurity risk. OECD *Future Global Shocks*. http://www.oecd.org/dataoecd/3/42/46894657.pdf.

Stiennon, R. (2010). *Surviving Cyberwar*. Lanham, Maryland: Government Institutes.

Tikk, E., K. Kaska, K. Rünnimeri, M. Kert, A.-M. Talihärm, and L. Vihul (2008). Cyber attacks against Georgia: Legal lessons identified. *NATO Cooperative Cyber Defense Centre of Excellence*. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

von Clausewitz, C. (1980 [1832]). *Vom Kriege*. Berlin: Ullstein.

Weiss, G. W. (1996). The Farewell Dossier. *Studies in Intelligence 39*(5), 121–126.

Woltag, J.-C. (2010). Cyber warfare. In R. Wolfrum (Ed.), *The Max Planck Encyclopedia of Public International Law (online edition)*. Oxford: Oxford University Press.

Legal framework and policy documents

Charter of the United Nations and Statute of the International Court of Justice, 1945, http://treaties.un.org/doc/Publication/CTC/uncharter.pdf

Congressional Research Service, *Cybersecurity: Authoritative Reports and Resources*, CRS Report for Congress, 26 April 2012, http://www.fas.org/sgp/crs/misc/R42507.pdf

Council of Europe, *Convention on Cybercrime*, ETS 185, November 2001, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, CETS No. 030, April 2959, http://conventions.coe.int/Treaty/EN/Treaties/html/030.htm

Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, http://www.unhcr.org/refworld/docid/3ddca4e14.html

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supplement No. 10 (A/56/10), chp.IV.E.1, November 2001, http://www.unhcr.org/refworld/docid/3ddb8f804.html

Ministry of Foreign Affairs of the People's Republic of China, *International Code of Conduct for Information Security*, proposal submitted to the 66th session the U.N. General Assembly, 12 September 2011, http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm

NATO, *Active Engagement, Modern Defence. Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, 19 November 2010, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 8 June 1977, http://www2.ohchr.org/english/law/protocol1.htm

Report on the Implementation of the European Security Strategy – Providing Security in a Changing World, S407/08, 11 December 2008, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

UN General Assembly Resolution 58/199 *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, 30 January 2004, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf

U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, strategic guidance document, January 2012, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

U.S. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, 13 February 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, December 2006, http://www.dod.mil/pubs/foi/joinet_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

U.S. National Security Strategy, May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Technical resources

F-Secure, *Stuxnet Redux: Questions and Answers*, 23 November 2010, `http://www.f-secure.com/weblog/archives/00002066.html`

McAfee, *Protecting Your Critical Assets. Lessons Learned from "Operation Aurora"*, March 2010, `http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf`

SANS Institute, *Bots & Botnet: An Overview*, 8 August 2003, `http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299`

Symantec, *IP Spoofing: An Introduction*, 11 March 2003, `http://www.symantec.com/connect/articles/ip-spoofing-introduction`

Symantec, *W32.Stuxnet Dossier*, February 2011, `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`

Schneier on Security (Bruce Schneier's blog), `http://www.schneier.com/`

The Lawfare Blog, `http://www.lawfareblog.com/`

List of Figures

Image Credits

Fig. 1: Patrick Chappatte, 30 May 2007, *International Herald Tribune*

Fig. 2: Randall Munroe, 1 August 2011, *xkcd*, `http://xkcd.com/932/`

Fig. 3: South Ossetia Hack Crew, 11 August 2008.

List of Acronyms

CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CISPA	Cyber Intelligence Sharing and Protection Act
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DoD	Department of Defense
DoS	Denial of Service
DST	Direction de la Surveillance du Territoire [Directorate of Territorial Surveillance]
FBI	Federal Bureau of Investigation
GCHQ	Government Communications Headquarters
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
JCS	Joint Chiefs of Staff
KGB	Komitet Gosudarstvennoy Bezopasnosti [Committee for State Security]
LAN	Local Area Network
LOAC	Law of Armed Conflict
Mbps	Megabit per second
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SQL	Structured Query Language
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
USB	Universal Serial Bus

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisor, Professor Hanspeter Neuhold. Your enthusiasm, support, and expertise – and not the least your unique sense of humour – have made it a real pleasure to work with you.

I would also like to thank the faculty and staff of the Diplomatic Academy for providing such a stimulating environment for my studies and research. I am especially indebted to Ambassador Hans Winkler for his encouragement and support, and to Professor Thomas Row for our many enriching conversations.

This thesis would not have been possible without the many individuals whose insights have helped shape my understanding of our changing world over the years – in all-night coding sessions, over gallons of coffee and *Club Mate*, through countless emails, tweets and IM sessions, and at the ephemeral but crucial random encounters at conferences, airports, and hotel lounges that seem to be such an essential part of our modern nomadic life style. In particular, I would like to thank Mathieu Baudier, Rafik Dammak, Marcin de Kaminski, Éireann Leverett, Morgan Marquis-Boire, René Pfeiffer, Eleanor Saitta, and Josh Shahryar for their input and inspiration.

Special thanks to Colonel (GS) Walter Unger of the Austrian Armed Forces Security Agency and Mag. Peter Gridling of the Federal Agency for State Protection and Counterterrorism for taking time out of their busy schedules to share their inside perspectives on dealing with high-level cyber threats in the real world.

I had the honour of being granted the Sobolak scholarship for the second year of my studies – *ein herzliches Dankeschön* to Peter Sobolak for his generous support!

At some point I was close to getting cabin (reading room?) fever. My friend Dana Vyzinkarova offered me asylum at her place, and we spent a very fun and productive week in Bratislava. It was during that time that the first draft of this thesis took shape. Thank you, Dana. (And watch out for those Bavarian spy pigeons!)

Finally, my deepest gratitude goes to my Mum. I would not be here without your unwavering love, support and belief in me. This work is dedicated to you.

Abstract

This thesis presents a critical contribution to the cyberwar debate, arguing that the notion of cyberwar is in fact ill-suited to dealing with the real cyber security threats we are facing.

One of the problems with the contemporary debate on cyberwar is the conflation of different cyber attacks. I therefore explain threats such as DDoS, website defacement, and SCADA attacks. I also discuss the various actors that make use of cyber attacks, ranging from criminals to hacktivists to violent state or non-state actors.

In addition to technical distinctions, the legal framework is important as well. If a cyber attack constitutes an act of war, the victim state has the right to retaliate by using armed force. The vast majority of cyber attacks do not fall into that category though, and thus are appropriately dealt with as matters of law enforcement.

I analyse a number of cases that are often cited as examples of cyber warfare, including the DDoS attacks on Estonian websites in 2007, the series of cyber incidents in Georgia in 2008, and the cyber attack on Google in 2009. For each of these cases, I discuss whether it qualifies as an act of cyberwar or not. A detailed case story deals with the Stuxnet worm that is widely considered to be an act of cyberwar by Israel and the U.S. against the nuclear enrichment facility in Natanz in Iran.

I consider it unlikely that a true cyberwar will take place. I base this assertion on the fact that significant cyber attacks are more difficult than commonly assumed, and that any actual acts of cyberwar would be likely to quickly lead to an escalation to kinetic conflict.

Based on these observations, I propose that cyberwar may not be the appropriate concept to address cyber security threats. The vast majority of cyber attacks that we have seen are not acts of (cyber) war but fall into the domain of (cyber) crime. The best way to deal with them is thus not a military response but a civilian one.

I conclude by presenting a number of recommendations for how to improve cyber security. These include encouraging a wider public debate, strengthening international efforts to fight cybercrime, improving the awareness about IT security in general, focusing on resilience, and introducing smart regulations to protect critical infrastructure.