Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyber Conflicts in International Relations: Framework and Case Studies

Alexander Gamero-Garrido
Engineering Systems Division
Massachusetts Institute of Technology
gamero@mit.edu | agamerog.mit@gmail.com

Executive Summary

Overview

Although cyber conflict is no longer considered particularly unusual, significant uncertainties remain about the nature, scale, scope and other critical features of it. This study addresses a subset of these issues by developing an internally consistent framework and applying it to a series of 17 case studies. We present each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. The profile of each case includes the actors, their actions, tools they used and power relationships, and the outcomes with inferences or observations. Our findings include:

- Cyberspace has brought in a number of new players – activists, shady government contractors – to international conflict, and traditional actors (notably states) have increasingly recognized the importance of the domain.
- The involvement of the private sector on cybersecurity ("cyber defense") has been critical: 16 out of the 17 cases studied involved the private sector either in attack or defense.
- All of the major international cyber conflicts presented here have been related to an ongoing conflict ("attack" or "war") in the physical domain.
- Rich industrialized countries with a highly developed ICT infrastructure are at a higher risk concerning cyber attacks.
- Distributed Denial of Service (DDoS) is by far the most common type of cyber attack.
- Air-gapped (not connected to the public Internet) networks have not been exempt from attacks.
- A perpetrator does not need highly specialized technical knowledge to intrude computer networks.
- The potential damage of a cyber strike is likely to continue increasing as the Internet expands.

- The size of the actor under attack could have an influence on its ability to deter the attackers with actions in the physical world.
- The entrance barriers (including the monetary cost) for any actor to get involved in a conflict seem to be much lower in the cyber domain than in the physical domain.
- Accountability on the Internet is difficult, and gets further obscured when the attacks transcend national borders. This fact has probably made cyber attacks desirable for major military powers such as China, Russia and the United States.

In many ways, this paper is a re-analysis of the case studies set presented on *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* recently published by the Atlantic Council. In addition, we draw upon other materials (academic and media) to expand our understanding of each case, and add several cases to the original collection resulting in a data set of 17 cyber conflict, spanning almost three decades (1985-2013). Cuckoo's Egg, Morris Worm, Solar Sunrise, Electronic Disturbance Theater, ILOVEYOU, Chinese Espionage, Estonia, Russo-Georgian war, Conficker, NSA-Snowden, WikiLeaks and Stuxnet are some of the major cases included.

Method And Organization

This study presents each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. Emphasis is placed on characteristics of cyberspace visible on conflicts.

Present work is divided in several sections. Part I presents the cases in terms of the actors involved, their power relationship, main actions, layers of the Internet affected, and outcome. Part II expands on the tools and instruments used on the cyber offensive and defensive actions described on Part I, including an extended view of the layers of the Internet affected. Part III presents the author's inferences and observations for each case, highlighting features of cyber conflict. Part IV presents a set of conclusions highlighting critical features related to: actors, socio-political context, tools and other technical issues, sophistication of the attacks, outcome and damage, and accountability.

Countries Involved

Findings presented in this study are U.S.-centered, as this paper was developed using such a focus. However, 23 countries are involved in at least one case, either in attack or defense. Countries involved in two or more cases are (frequency in parenthesis): United States (16), Russia (7), China (3), Israel (3), The Netherlands (2) and Germany (2). Six of the cases presented had a global reach.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyber Conflicts in International Relations: Framework and Case Studies

Alexander Gamero-Garrido
Engineering Systems Division
Massachusetts Institute of Technology
gamero@mit.edu | agamerog.mit@gmail.com

Abstract

Twenty years ago, the possibility of having an international conflict extend into the cyber domain was distant. Since then much has changed. Today cyber conflict is not considered particularly unusual. But considerable uncertainties remain about the nature, scale, scope and other features of such conflicts. This paper addresses these issues using a re-analysis of the case studies presented in *A Fierce Domain* recently published by the Atlantic Council. In addition, we draw upon other materials (academic and media) to expand our understanding of each case, and add several cases to the original collection resulting in a data set of 17 cyber conflict, spanning almost three decades (1985-2013). Cuckoo's Egg, Morris Worm, Solar Sunrise, EDT, ILOVEYOU, Chinese Espionage, Estonia, Russo-Georgian war, Conficker, NSA-Snowden, WikiLeaks and Stuxnet are some of the major cases included. This study presents each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. The profile of each case includes the actors, their actions, tools they used and power relationships, and the outcomes with inferences or observations. Emphasis is placed on characteristics of cyberspace visible on conflicts. Findings include: Distributed Denial of Service is the most common offensive action; accountability is difficult in cyberspace, particularly with international conflicts; outcomes of each instance have been variable, and economic impact is hard to estimate; the private sector has been a key player in cybersecurity; size of an actor, and countries' ICT infrastructure, influence the nature of the cyber conflicts.

Acknowledgement: This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

About the author: Alexander Gamero-Garrido is an SM candidate in Technology and Policy at the Engineering Systems Division, Massachusetts Institute of Technology. He holds an Engineer degree from Universidad Simón Bolívar in Caracas, Venezuela, and did a master thesis at the School of Engineering at Lund University, Sweden. He is a research assistant for Prof. Nazli Choucri at the Department of Political Science at MIT, co-advised by Senior Research Scientist David Clark at the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT. His research is focused on international cyber conflict, and the relationship between policy, privacy and Internet architecture. Before MIT he worked in oil exploration, and has received awards or funding from Fundación Carolina, Fundación Rafael del Pino and Fundación Santander (Spain), Cato Institute (USA), USB, UCAB, IESA and Fundación Futuro Presente (Venezuela).

Acknowledgements: the author would like to thank Nazli Choucri, Professor of Political Science at MIT, for her valuable insights. Additional thanks to Elizabeth Nigro.

Table of Contents

Introduction

Just twenty years ago, the possibility of having an international conflict extend into the cyber domain was very distant. Relatively recent events, such as the cyber attacks in Estonia in 2007, or Stuxnet, have changed that landscape, shaping what is now known as cyber conflict.

This paper focuses largely on a set of cases presented in *A Fierce Domain*, recently published by the Atlantic Council [13]. To provide greater depth, we transcend the analysis based on materials in other sources. In addition, we examine several cases not included in the initial body of cases in order to obtain wider coverage.

In many ways this study is a "re-analysis" designed to develop an internally consistent view of cases examined based on a common framework. This framework consists of:

- Sociopolitical context of each case in its socio-political context,
- Technical details of the attacks, including the tools and instruments used,
- The outcome of the case (including policy changes, damage, prosecution, international reactions as relevant).
- Based on the above, we then derive some inferences from this wide range of cases in order to identify characteristic features and highlight facts inherent to conflict in cyberspace.

Appendix 2 to this paper summarizes the analysis and the results in easily readable and concise matrix.

1. Cases Defined

Cyber conflict as used in this paper is a wide term that spans from low-level intrusions, such as petty crime to create spam networks all the way to high-scale, state-sponsored cyber warfare. We expect the analysis to provide some evidence about the types of damages that are done, and the tools used to create the damages.

The series of case studies involves analysis and comparison of 17 cases. Each case focuses on the actors involved, the tools used to exert action, the power relationship among them, the outcome, and inferences and observations, the two latter by the authors. These cases of cyber conflict include any form of cyber confrontation transcending national borders. The time frame is between 1985 and 2013.

The cases are listed in Table 1, along with their date of occurrence, in chronological order. In this table, two of the last cases presented (15 and 16) correspond to individual-initiated leaks of classified (or otherwise secret) information pertaining to the United States: Wikileaks and Edward Snowden's revelations on NSA surveillance.

Table 1. List of cases presented and dates of occurrence.

Case number and case name	Date
1. Markus Hess hacks into several US military and research facilities (Cuckoo's Egg)	August 1985
2. Morris Worm	November 1988
3. Dutch Hackers and British Hackers	1990-1994
4. Operation Solar Sunrise	Feb 1998
5. Moonlight Maze	March 1998
6. Electronic Disturbance Theater (EDT) attacks Pentagon	September 1998
7. ILOVEYOU and several other worms released	Circa 2000
8. "Patriotic Hackers" Attacks	1999-2001
9. Chinese Cyber Espionage	2005-2012
10. Estonia receives cyber attacks	April 17th to May 18th, 2007
11. The Russo-Georgian War and its cyber component	2008
12. Agent.btz infects US classified and unclassified networks, leading to operation Buckshot Yankee to counter it	2008
13. Conficker Worm began to spread	November 2008
14. Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic Games)	2009-2010
15. Wikileaks releases thousands of diplomatic cables pertaining to the US State Department and its Missions abroad	2010-2011
16. Edward Snowden leaks information about NSA classified mass surveillance programs	2013
17. Hackers Intrude into New York Times	2012-2013

We now present list of countries and international organizations involved in at least two cases and their frequency of appearance. "Country" does not necessarily imply state[1]; if the party under attack or the attacker were in a determined jurisdiction, the relevant case

[1] *A Fierce Doman* [13, pp 265-278] presents a methodology for determining the likelihood for a State to be involved in an attack, with several cases as examples. Our approach is different in the sense that evidence indicating State-sponsored attack or defense is included in the relevant category of our own methodology described in this section. In particular, hard evidence is treated differently than inferences and observations. The latter are included in Part III, while the former is included in Parts I and II.

is associated with that jurisdiction ("country"). They are listed from most frequent to least frequent.

1. United States (16 cases)
2. Russia (7)
3. NATO (3)
4. China (3)
5. Israel (3)
6. The Netherlands (2)
7. Germany (2)

Figure 1 presents the cases in which each of the countries listed above is involved. For a complete overview of countries and international organizations involved in each case, please see Appendix 4.

Country or International Organization	Private sector	United States	Russia	Global reach	China	Israel	NATO	The Netherlands	Germany
Case number and name									
1. Cuckoo's Egg	x	x	x						x
2. Morris Worm	x	x		x					
3. Dutch Hackers and British Hackers		x						x	
4. Operation Solar Sunrise	x	x				x			
5. Moonlight Maze	x	x	x						
6. Electronic Disturbance Theater (EDT)	x	x							
7. ILOVEYOU	x	x		x					
8. Patriotic Hackers	x	x	x		x		x	x	
9. Chinese Cyber Espionage	x	x		x	x				
10. Estonia receives cyber attacks	x		x			x	x		x
11. The Russo-Georgian War	x	x	x						
12. Agent.btz and operation Buckshot Yankee	x	x	x				x		
13. Conficker	x	x		x					
14. Stuxnet, Flame and Duqu	x	x				x			
15. Wikileaks	x	x		x					
16. Edward Snowden's NSA leaks	x	x	x	x					
17. Hackers Intrude into New York Times	x	x			x				
Frequency	**16**	**16**	**7**	**6**	**3**	**3**	**3**	**2**	**2**

Figure 1. Countries involved in at least two cases, the cases in which they are involved and their frequency of appearance.

Figure 2 presents the number of cases per country or jurisdiction on a global map, generated using TargetMap [115].

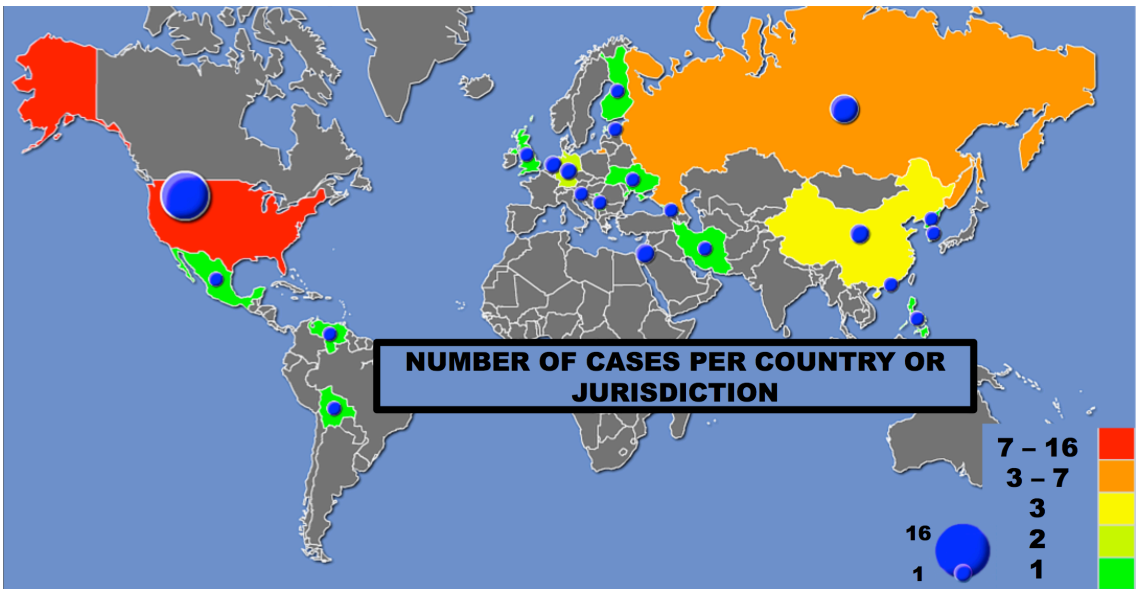

Figure 2. Map: number of cases per country or jurisdiction, generated using TargetMap web application [115].

2. Method of Analysis

The method we have used consists of the following steps:

1. Identify the *case* (most of them come from a timeline available on [13] website at the Atlantic Council: acus.org/afiercedomain). This step generated Table 1. In addition, we covered cases numbered 13 (Conficker), 15 (Wikileaks), 16 (NSA leaks) and 17 (New York Times) that were not part of the *Fierce Domain* data set.

2. Identify the *actors* in each case, whether they are State, private organizations or individuals; and to highlight any unusual features. That information yielded a view of the "actors" feature of each case. This information is included in Part I.

3. Identify the *actions and tools used* directly undertaken by the actors, notably, internal or indirect actions as relevant. These actions included the tools or instruments used, and the layers of the Internet they affected.

4. This allows us to generate a view of the *power relationships*,

Jointly, the above allows us to obtain a "*big-picture"* view of each case and provided information about the socio-political context at the time.

If a pattern or trend is detected that connects more than one case; or if there are major implications spinning directly off the case, e.g. a new policy directive or the formation of an organization; or if there is a situation which can be extrapolated and generalized; among others, then we can generate the *outcome and inferences* also.

Based on the above, we present our own inferences and observations. Particular attention is paid to characteristics inherent or unique to cyberspace-based actions (such as, for example, difficulties in accountability).

As a general rule we consulted a range of sources from academic journals for technical details, and socio-political context in order to build a richer view of the outcome of the case (including policy changes and policymakers' actions), and lessons learned. We consulted articles in the media as well as other web sources for damage estimates (financial losses or other), and tools used by attackers. Media sources were also used for socio-political context, prosecution of attackers, relevant events taking place concurrently to the case, and policymakers' actions.

The method applied yielded a matrix with the cases and all the above-described information. For reference, it is included as Appendix 2.

Appendix 1 presents a brief set of actions or exercises related to cybersecurity in the United States, as described on [13]. Appendix 3 includes the definition of cyberspace layers used on Part II. Appendix 4 presents an overview of countries and international organizations involved in each case. Appendix 5 presents a preliminary list of cases that will be included in a future paper, and analyzed using the methodology described here.

3. Organization

This paper is organized in several sections. Part I presents the cases in terms of the actors involved, their power relationship, main actions, layers of the Internet affected, and outcome. Part II expands on the tools and instruments used on the cyber offensive and defensive actions described on Part I, including an extended view of the layers of the Internet affected. Part III presents the author's inferences and observations for each case, highlighting features of cyber conflict. Part IV presents a set of conclusions highlighting critical features related to: actors, socio-political context, tools and other technical issues, sophistication of the attacks, outcome and damage, and accountability.

PART I

The Cases: Actors, Power Relationships, Actions and Outcome

Here we present the cases in chronological order. Each case is examined in the same way so that we can build an internally consistent set of conclusions. For a detailed analysis of tools used and layers of the Internet affected, see part II.

1. Cuckoo's Egg – August 1985

The earliest event included in this study, Cuckoo's Egg is relevant given the relatively low development of the Internet at the time (August 1985) and the high level of the facilities affected: several military and research facilities in the United States [64].

Actors Involved

- Markus Hess / German citizen working for KGB [64].
- Clifford Stoll / Systems Administrator for Berkeley Lab [64].

Actions

Hess intruded military and research facilities in the United States and was detected, monitored and deterred by Stoll [64].

Affected Layers of the Internet

Physical.

Power Relationships

Stoll had difficulties attracting attention to the case from officials, since they were "more concerned with 'real' crime and counterintelligence than the hard-to-fathom world of networks." [13, p7]

Outcome

Hess and associates obtained "sensitive semiconductor, satellite, space, and aircraft technologies" from higher education and military institutions in the U.S. [3]

2. Morris Worm – November 1988

Actors Involved

- Robert Tappan Morris [5]
- Cornell University [5]

Actions

Morris released a worm from MIT; the worm spread rapidly and caused significant Denial of Service damage and cleanup costs [4].

Affected Layers of the Internet

Physical and Application.

Power Relationships
This was most likely a one-man-act and was duly condemned by the Cornell University commission who investigated the case: "This was not a simple act of trespass analogous to wandering through someone's unlocked house without permission but with no intent to cause damage. A more apt analogy would be the driving of a golf cart on a rainy day through most houses in a neighborhood. The driver may have navigated carefully and broken no china, but it should have been obvious to the driver that the mud on the tires would soil the carpets and that the owners would later have to clean up the mess." [5]

Outcome
A relatively large fraction of the computers connected to the Internet at the time were infected (some quote 10% [70]).

The Cornell commission investigating the case fended off attempts to portray Morris's actions as heroic: "Although such security flaws may not be known to the public at large, their existence is accepted by those who make use of UNIX." [5] Morris was sentenced to 3 years probation, 400 hours of community service and fined $10,000 [79].

As a result of the above, the U.S. Department of Defense (DoD) funded the creation of the first-ever Computer Emergency Response Team (CERT) at Carnegie Mellon University [13, p32].

3. Dutch and British Hackers – 1990-1994

Actors Involved
- Unnamed Dutch "teenage hackers" [6].
- US Military.
- North and South Korean installations [13, p37].

Actions
Dutch hackers "intruded into the networks of 34 US military installations during the lead up to the first Gulf War." [55] British hackers attacked South Korean targets [13, p37].

Affected Layers of the Internet
Information.

Power Relationships
USDA website [6] states that no foreign intelligence agency was proven to be involved.

Outcome
The "[teenagers from Holland] using fairly unsophisticated methods… were searching for information on missiles, nuclear weapons, and DESERT SHIELD." [55] They gathered information for "over a year" regarding US operations prior to the Gulf War [6].

The US military didn't know for hours if the target was in North or South Korea, and if it were to be the former it could have been interpreted as a threat by the regime, at the time in negotiation with the US regarding their nuclear program [13, p37]. The target was, however, in South Korea [13, p37].

4. Operation Solar Sunrise – February 1998

Actors Involved

- Two teenagers from California and one teenager from Israel (Tenenbaum) [65].
- Military agencies in the US and Israel.

Actions

The attackers intruded government sites in the United States (including the Pentagon) and Israel [65].

Affected Layers of the Internet

Logical and Information.

Power Relationships

This attack had apparent massive mobilization due to the suspicion of 'Iraqi warfare' and went all the way up to the U.S. President's Office [9].

"Although all DoD targeted systems were reported as unclassified, many key support systems reside on unclassified networks (Global Transportation System, Defense Finance System, medical, personnel, logistics, and official e-mail)" [67]

Tenenbaum, the Israeli teenager, claims his objective was to "show the systems' vulnerability" rather than to cause harm [65]. He was later convicted for credit card fraud [66] in an unrelated incident.

The U.S. had ongoing tensions with Iraq at the time [65]. The former suspected the attacks came from the latter, but found the Californian teenagers instead. [13, p43] [105]

Outcome

This real world incident led to the creation of the Joint Task Force for Computer Network Defense (JTF-CND) by the US Department of Defense [13, p44-47]. For the first time there was a centralized unit capable of (and responsible for) responding to cyber attacks "crossing borders between commands and agencies" [13, p44-47].

The JTF-CND would initially report directly to the Secretary of Defense, although it was moved under the US Space Command within a year [13, p44-47].

An interesting feature of the JTF-CND was the coordination with the private sector in "critical industries" via the National Infrastructure Protection Center (NIPC) [13, p44-47].

JTF-CND's mission was expanded to potentially include Offense, renaming it to JTF-CNO, with the last "O" standing for Operations [13, p44-47].

The outcome of the attack was consistent with the findings of operation Eligible Receiver (see Appendix 1): "DoD has no effective indications and warning system, intrusion detection systems are insufficient, DoD is not organized effectively for IO, and that identifying the threat group and motives is a problem." [79]

5. Moonlight Maze – March 1998

Actors Involved

- "Russian cyber-spies" [68].
- United States' National Infrastructure Protection Center (NIPC) and Joint Task Force for Computer Network Defense (JTF-CND) [69].

Actions

Russian spies intruded the United States military, agencies and "leading civilian universities." [68] The National Infrastructure Protection Center (NIPC) and the Joint Task Force for Computer Network Defense (JTF-CND) coordinated "Corrective" actions [69].

Affected Layers of the Internet

Information.

Power Relationships

Details remain classified, but according to a professor in the area the attacks were traced back to Russia, although he admits that this is no indication of the source of the attack [81].

This turned out to be a high profile case resulting in a "wake-up call to the DoD". In DoD's words "Defense exercises and real world events in 1997 and in early 1998 demonstrated the need for an organization within the Department to coordinate its defensive activities and to have the authority to direct the necessary actions for that defense."[82]

The Secretary of Defense called this a "state sponsored attack" [13, p49]. At the very least, it showed the potential impact of a specialized, potentially state-backed, attack – as opposed to a random attack by some individuals with rather unclear goals.

Outcome

John Arquilla, a professor of defense analysis, says regarding this incident "In the realm of cyberspace-based disruptive threats, we haven't yet had what they call the electronic Pearl Harbor" [70]. "What we really are talking about is a social gulf between those who have the skills to do costly disruption and those who are radical enough to want to do it." [70]

Shortly after Moonlight Maze, Presidential Decision Directive 63 (PDD-63) "sets a goal of a reliable, interconnected, and secure information infrastructure by the year 2003." [81] Also, "The National Infrastructure Protection Center (NIPC) was established as a result of PDD-63" [81]. The DoD's Joint Task Force for Computer Network Defense came operational that same year [13, p48].

The same year this happened a group of hackers testified in front of the Governmental Affairs Committee of the US Senate [36]. An interesting conclusion of that hearing is that there were not many incentives for software companies to increase security in their systems. According to the testimony, "companies want to ignore problems… it's cheaper

for them." The hackers also emphasized the difficulty of establishing where or from whom a particular action is coming from on the Internet [36], a fact consistent with Moonlight Maze's outcome.

6. Electronic Disturbance Theater (EDT) attacks Pentagon – September 1998

Actors Involved

- Electronic Disturbance Theater (EDT) – a group of activists [63] on the cyber domain.
- The United States and Mexico.

Actions

EDT developed and released tools to attack sites in the United States and Mexico, and coordinated the attacks [61][63]. Target sites used defensive measures in order to deter the attackers [106].

Affected Layers of the Internet

Physical and Logical.

Power Relationships

In their website, EDT claims to be "engaged in developing the theory and practice of Electronic Civil Disobedience (ECD)." [63] Ricardo Dominguez, an associate professor at the University of California San Diego [62], led the EDT.

Outcome

The socio-political nature of this attack is consequent with "Dorothy E. Denning's testimony before the U.S. House of Representatives: 'Both EDT and the Electrohippies view their operations as acts of civil disobedience analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction.'" [71]

EDT represents a novel form of protest: "While maintaining a focus on the Zapatista movement--paradoxically, a nomadic site-specificity-- EDT has realized the (potential) links between bottom-up struggles for social justice." [71]

7. ILOVEYOU and several other worms released – Circa 2000

Actors Involved

- ILOVEYOU was developed in the Philippines by, among others, a former computer science student, Onel de Guzman. [14] [15]
- Philippines's National Bureau of Investigation (NBI), with the assistance of the U.S. FBI [15]
- Microsoft [23].

Actions

De Guzman developed and released ILOVEYOU, which went to infect a significant portion of the Internet through Microsoft Outlook, an email client [16][23]. He was investigated by the NBI [15], but was not convicted [14].

Affected Layers of the Internet
Information, logical and Physical.

Power Relationships
ILOVEYOU affected tens of millions of computers worldwide and had an estimated clean-up cost of USD 15 billion. [17]

Despite this dramatic impact, the charges against the suspects were dropped: there was no law in the Philippines at the time punishing the development of malware [109].

There was no international treaty that would enable the prosecution of de Guzman. The ILOVEYOU episode increased awareness on the need to coordinate prosecutions internationally – given the nature of cyberspace, i.e. transcending "constraints of geography and physical location"[24, p3]. See [18] for a review of some of the international initiatives under way in 2002, including actions by the European Union and G-8.

Onel de Guzman left school when his department rejected his thesis [15]. His work consisted in a proposal to massively steal passwords, in order to allow more people to connect to the Internet [15].

Outcome
This worm was, given its massive reach, a wake-up call to a number of actors, including technology giants such as Microsoft [23]: "ILoveYou grabbed the entire world, for the first time, by the collar and forced it to take security seriously" [16].

The author –or one of them– of Melissa (an American citizen), a virus which spread about a year earlier than ILOVEYOU, was sentenced to 20 months in prison, fined USD 5,000 and ordered to "not be involved with computer networks, the Internet or Internet bulletin boards unless authorized by the Court" [21]. By comparison, one of the authors of ILOVEYOU, causing much more widespread damage than Melissa (which limited itself to the first 50 contacts in the address book [22]), could not be sentenced in the Philippines. Instead he was free to be interviewed and brag about how he had "become part of the history of the Philippines."[14]

This worm affected a large number of private actors. According to McAffee, then the largest antivirus vendor, the worm infected "60 to 80 percent of its Fortune 100 clients." [22]

8. "Patriotic Hackers" Attacks – 1999-2001

Actors Involved

- The United States and its North Atlantic Treaty Organization allies.
- Serb and Russian hackers [13, p50].
- American hackers [13, p50].
- Dutch hackers [13, p50].
- Chinese hackers [13, p50].

- China.

Actions
During the Kosovo war, hackers from the United States, Serbia, Russia, The Netherlands and China attacked sites belonging to the belligerents and related actors.

Affected Layers of the Internet
All layers: Physical, logical, information and user.

Power Relationships
These attacks are perhaps the first instance where the episode can be called a "cyberwar" [30], because they were connected to the ongoing physical war in Kosovo.

The US and Chinese responses to the cyber attacks originating from its territory were distinctly different. The former made it clear to its citizens that it did not encourage patriotic hacking, given that "such activity is illegal and punishable as a felony." China, on the other hand, did little to encourage its own hackers to stop [13, p51]. This is consistent with dissimilar views of the Internet as a tool for foreign policy [13, p50]. As a minimum, cyber attacks on foreign targets were seen very differently in the two countries.

Evidence suggests that at least some of the hackers here were regular citizens, presumably not involved in politics, the military or espionage, and with very limited actual political or military power. Cyberspace provided them with a venue to be actors in the war, with limited risks and a very visible outcome.

Outcome
One main consequence of this series of episodes is the emergence of cyber as a domain for warfare. Although [13, p27-40] shows that the consideration of cyber defense since at least two decades before 1999, the potential consequences should Kosovo related attacks been more successful "could have been devastating"[35]; this in turn showed the world, and military powers in particular, that "the Internet is no longer just a side issue." [27]

Source [35] quotes that most of the attacks concerned in this case have been classified as cyber terrorism. The official response of the US was to shut down the DOE website until clarifying how the hackers managed to gain access [30]. The White House also closed its site for a few days largely as a preventative measure following hijacking attempts [30].

9. Chinese Cyber Espionage, 2005-2012*· [13, p165-173]

Actors Involved
- China. Agencies include "the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Second Department of the People's Liberation Army General Staff Department (2PLA), or the Liaison Office of the General Political Department." [42].

*· These dates mark the first public U.S. recognition of the Chinese intrusions and the latest time for which this case's sources address the issue; this is believed to be an ongoing threat [13, p173].

- Hacker groups based in China.
- The United States, its allies, and over a hundred countries as the targets of the attacks [13, p167].
- Private firms in diverse economic sectors, mostly in technology.

Actions
Mainland China-based groups perpetrated intrusions into systems in the United States, its allies, and other countries, both for commercial and State-sponsored espionage.

Affected Layers of the Internet
Information.

Power Relationships
The head of the US National Security Agency and Cyber Command has estimated the loss for American companies in intellectual properties at USD 250 billion per year [13, p173]. This is an enormous incentive to denounce and try to stop the Chinese espionage.

That, however, has not been the case, with few exceptions such as Google denouncing what has been called "operation Aurora" [94].

There might be a number of reasons for the above. In the private actors case, denouncing China could lead to Beijing making it harder for them to do business there [13, p173]. Considering rapid Chinese economic expansion, and the fact that the middle class there is larger than the entire population of the United States [37], is arguably a strong incentive not to publicly denounce Chinese intrusions.

The US and China, as the world's two biggest economies [38], are also economically interdependent. Only in US Treasury Bonds, China is reported to own USD 1.25 trillion [39]. This, and the need for cooperation in geopolitical issues such as Syria and Iran [13, p173], may complicate US government public attempts at denouncing Chinese cyber espionage.

APT1, a Chinese hacking group, has major infrastructure including "1,000 servers" and a "special fiber optic network" [99].

Unconventional agents include ethnic Chinese not physically present in China [42]. However, there seems to be a bias in the literature towards believing this group to be the majority, while in reality that might not be the rule but rather an exception that mainly targets political dissidents or Taiwan [42].

Outcome
Companies might have other reasons for not defying China publicly: although the intellectual property fight seems to be rising in the United States [40], fighting that fight in China may be more difficult; besides the inherently different Chinese framework for intellectual property [41], there might be little gain in trying to prosecute a Chinese hacker and recover the loss, since any enforcement would require diplomatic efforts [33], which may not be available but for the largest companies.

There is a distinction to be made on what is generally qualified as "Chinese espionage."[42] The "conventional view" for Western analysts tends to categorize most types of espionage as if being State-sponsored [42]. In reality, the main goal of Chinese "official" intelligence is to protect the power of the Communist Party [42]. The highlight is that non-state actors also execute economic espionage, with or without official Chinese support or encouragement [42].

The Cox Report, the result of a US House of Representatives commission, concluded that China had gained access to "advanced US thermonuclear weapons."[43]

A small California-based company (Cybersitter) claims its software was basically stolen by the Chinese government for use in the Green Dam Project, the massive firewall preventing millions of Chinese users to access contents ranging from pornographic sites to politically oriented portals [33]. The company states the Chinese government owes it USD 2.2 billion [33]. The suit, however, had limited chance of success because it was done in a U.S. court, with the alleged criminal activities taking place in China [33]. Following the suit, the company received a cyber attack, presumably from China [34].

The Chinese hacking group identified by Mandiant (a cybersecurity firm) as APT1, is involved in economic espionage, attacking companies in many industries, and stealing commercial information [98][99].

10. Estonia receives cyber attacks from April 17th to May 18th, 2007 [13, p174]

Actors Involved

- Estonia.
- Russia.
- Estonian private actors, including newspapers, technical associations, banks and individuals.
- Public and private actors from NATO allies, particularly Finland, Israel, Germany and Slovenia [13, p184] [46].
- Russian and Russian-Estonian hackers, and members of the Russian diaspora worldwide, possibly supported by the Kremlin.

Actions

Following an ongoing political controversy over a World War II monument, Russians conducted a series of attacks to official and commercial websites in Estonia.

Affected Layers of the Internet

All layers: Physical, logical, information and user.

Power Relationships

The motivation for the attacks can be traced perhaps to earlier in 2007, when Estonia had announced it would move a WWII monument (the Bronze Soldier [48]) from the center of its capital Tallinn to a cemetery in the outer edge of the city [13, p174-176]. The

monument carried strong symbolism for ethnic Russians living in Estonia and Russians alike, as it represented the Soviet victory over Nazi Germany (Russian decision-makers asked Estonia not to move the monument) [13, p174-176]. For some other Estonians, however, the monument was a symbol of Russian oppression during the USSR regime [13, p174-176] (Estonia became independent only six years earlier in 1991) [56].

As Estonia qualified the attacks as being of Russian origin, International cooperation, including several European countries and Finland in particular, arose [13, p184-186]. This included individual foreign technical professionals, ISPs, network companies, and other private and public actors [13, p184-186]. The attacks were traced back to Russia, but the direct involvement of the Kremlin has not been proven [13, p189-190]. The price of hiring a botnet with sufficient bandwidth to perform the attacks was $75/day [13, p183].

This did not stop, however, Estonian politicians and senior media officials of attacking Russian government directly in the aftermath of the attack, and the event "continues to frame Russian-Estonian relations today." [13, p188-189] The Estonian reaction may have been directed at discouraging future uses of cyber attacks to exert influence in international relations, particularly by Russia [13, p184-191].

Although for the context of this paper the cyber attacks are the central issue, the physical counterpart during the concerned period was present in the form of riots and street violence [46]. Even though the actual perpetrators of the DDoS attacks were also located outside Estonia (presumably members of the Russian diaspora [46]), these actions were a part of an ongoing clash among different ethnic populations (Russian and Estonian) in Estonia.

Generally speaking, Estonia was an ideal target for a cyber attack because of its advanced ICT infrastructure and widespread Internet use: "97 percent of bank transactions occur online; and in 2007, 60 percent of the country's population used the Internet on a daily basis." [46]

Outcome

Estonia became a cybersecurity hub in the aftermath of the attack, as shows the "hosting of the NATO Cooperative Cyber Defense Center of Excellence and EU Agency for large-scale IT systems." [13, p187]

The suspicions of Russia being involved directly are not irrational. Former Soviet states, such as Estonia, are of particular importance in Russian foreign policy, and diminishing Western influence [13, p191] in the region is a very likely goal of the Kremlin.

The volume of the attacks, and their coordination over time, also make Russia a viable suspect over an ad-hoc network of hackers in the Russian diaspora [13, p188-189] [46].

Use "of globally dispersed and virtually unattributable botnets" [46], and particularly those including computers used without the owner's knowledge (as was the case in Estonia) [47], obviously makes prosecution of the culprits very difficult: "Estonian

authorities made a few in-country arrests but never uncovered the main culprits, who were allegedly operating out of Russia" [46]. By contrast, 300 people had been arrested by the morning of the day after the street riots started [111].

11. The Russo-Georgian War, 2008 [13, p194] – and its cyber component

Actors Involved

- Russia.
- Russian organized crime.
- Georgia.
- Estonia and other NATO allies supporting Georgia.

Actions

The Russo-Georgian war had a cyber component, leading to the disruption of official and civilian websites in Georgia, following attacks by Russia.

Affected Layers of the Internet

All layers: physical, logical, information and user.

Power Relationships

The cyber conflict offensive was simultaneous with the ongoing Russian operation on South Ossetia, a disputed region in the north of Georgia; South Ossetian independence efforts are openly supported by the Kremlin [13, p194-196].

The period leading to the war saw military exercises conducted by Moscow in South Ossetia and Abkhasia (another disputed region) [13, p194-196]. Conversely, Georgia made efforts to step up its military force and conducted exercises with NATO, although the latter's "troops had already left before the fighting with the Russians began." [13, p194-196]

Although the direct involvement of Moscow was not (as in the attacks against Estonia) directly proven, "consider[ing] the forensic evidence, geopolitical situation, timing, and the relationship between the government, the youth, and criminal groups, it is not difficult to conclude that the Kremlin was behind it all"[13, p201]. This assertion is significant when Russia is considered one of the most powerful military powers in the world [52].

There are indications of the participation of Russian criminal groups, which may be related to the Kremlin [13, p200-202].

Estonia supported Georgia, but the scope of the attacks meant that they mostly did damage control [13, p199].

Outcome

The most palpable impact on the general population was the downtime of the banks' electronic systems, denying people in Georgia access to their money [13, p198]. See also [53], which provides a case for the application of International Humanitarian Law to the Russo-Georgian cyber conflict. The outcome of the war itself has been described on [13,

p196] as a "show of Russian superiority and the degradation of the long-term effectiveness of the Georgian military."

Appealing to nationalism, sites with a .ru [13, p201] (Russia) domain recruited, trained, and provided tools to new hackers in Russia and elsewhere. This has been called a cyber militia [13, p204]. It is in fact a Russian tactic goal to façade cyber attacks as of being of "criminal or terrorist" origin [13, p203]; similar cyber militia approaches have been taken by China and Iran [13, p204].

12. Agent.btz infects US classified and unclassified networks, leading to operation Buckshot Yankee to counter it, 2008 [13, p205]

Actors Involved

- The US Military.
- NATO.
- A "Russian foreign intelligence agency" (allegedly) [13, p206].

Actions

The virus Agent.btz infected classified and unclassified networks in the United States military. It reached air-gapped networks (not connected to the public internet).

Affected Layers of the Internet

Information.

Power Relationships

Senior US Officials, including President George W. Bush and Secretary of Defense Robert M. Gates were briefed on the incident [13, p209], speaking of its gravity.

The origin of the virus is uncertain; but "evidence suggests both that the US military is confident it knows who is responsible, and that it unofficially attributes a Russian foreign intelligence agency."[13, p207]

There is no report in [13, p205-211] of the virus causing significant damage. This may have been either because the virus couldn't receive further instructions from its creator, or because it was intended for information gathering.

Outcome

The incident led to a ban on thumb drives and other forms of removable media for over a year [13, p209]. This measure in itself is significant, since troops were reported to use such devices to transfer data when network resources are limited [13, p210].

According to [13, p210-211], Agent.btz and Buckshot Yankee changed the U.S. Military in several different ways:

- The NSA and the DoD began working together. In detecting and countering the virus, the NSA was a key player.
- The creation of the Cyber Command, and the subsequent change in the cyber "culture, conduct and capability."

- Cybersecurity was given a higher priority from this point forward.

13. Conficker Worm – Began to spread in November 2008 [58]

Actors Involved

- Cyber criminals, working for profit. (The exact origin remains unknown, but evidence points toward Ukraine [102]).
- The Internet security community.

Actions

The Conficker worm infected tens of thousands of computers worldwide, presumably to build a for-profit spam network ("botnet").

Affected Layers of the Internet

Physical, logical and information.

Power Relationships

Botnets can serve several purposes, ranging from petty cyber crimes such as spam, to State sponsored warfare actions [58]. Evidence suggests Conficker was used "as a platform for conducting wide-scale fraud, spam, and general Internet misuse" for profit [58], rather than any State sponsored cyber warfare.

Outcome

Conficker infected millions of computers [58], in over 180 countries [112], causing $ millions in damage [58]. Some of the vulnerabilities were patched by the software vendors, but this can only help if the infected computers are patched, which is not the case for a "huge worldwide pool of poorly managed and unpatched Internet-accessible computers." [58] The previous point highlights the need for a new security scheme of adaptation to dynamic (continuously adapting) security threats [58].

Whitehats, or hackers working on the cybersecurity side, created a new organization to deal with the widespread infection of Conficker, sharing technical knowledge and security insights with policymakers and the population at large [58].

14. Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic Games) 2009-2010[13, p212]

Actors Involved

- The United States.
- Iran.
- Iranian nuclear facility in Natanz.
- Israel.
- France and Germany (on nuclear issues, not the cyber attack).
- Symantec and other cybersecurity companies.

Actions

Flame, Duqu and Stuxnet were part of a cyber campaign led by the United States to disrupt control systems in Iranian nuclear facilities.

Affected Layers of the Internet
All layers: physical, logical, information and user.

Power Relationships
The initial purpose of Iranian nuclear program was to generate electricity and reduce the dependence on fossils [13, p213-215]. The United States, France and Germany supported this effort during the Shah's government. That support was dropped due to fears of Iran developing a nuclear weapon (the fear began before the Iranian revolution) [13, p213-215].

Clashes between Israel and Iran are not new. Former Iranian President Ahmadinejad has argued that Israel should disappear; therefore, Israel has sought support from the United States to counter Iranian nuclear weapon development [13, p216-217].

A conventional use of warfare was "politically risky", leading to the use of cyber attacks to deter Iranian nuclear program. [13, p216-217]

The technical complexity and extension of the virus, along with the highly specialized information on industrial systems needed to produce it, point out to a level of sophistication only attainable by nation-state agencies [13, p223]. Furthermore, the relatively low profile of the incident in the media, plus the specificity of the target, make anti-nuclear-weapons activists a very unlikely suspect [13, p223].

The New York Times and a "German security expert" both attribute the virus to the United States and Israel [13, p224]. They may have used their own nuclear facilities to test the virus, and information from Israeli Mossad to develop it [13, p226-227]. Edward Snowden has allegedly revealed that Stuxnet was the work of Israel and the United States [95].

Outcome
The incident damaged almost 1,000 centrifuge tubes [13, p218] in Iranian Natanz facility. This figure is significant in the light of the total number of installed tubes (9,000) and the portion of those fed with uranium (4,000) [13, p228]. "A 23% decline in the number of operating centrifuges from mid-2009 to mid-2010 may have been due to the Stuxnet attack." [57]

Iran created a new cyber unit in its militia [13, p229]. Not much later, Comodo, a US based security firm, accused Iran of attacking several Internet giants, including Google and Microsoft [13, p229].

Source [57] argues that Stuxnet used a blend of tools from the cyber crime community, and extends this to the cases in Estonia, Georgia and several others. The same paper uses that as an argument to downplay the technical sophistication of Stuxnet, its spreading mechanism, and its resilience. Furthermore, the use of third-party code increases the difficulty in the attribution of a cyber attack [57].

15. Wikileaks releases thousands of diplomatic cables pertaining to the US State Department and its Missions abroad 2010-2011

Actors Involved

- Wikileaks – a not for profit "transparency" organization founded and led by Julian Assange [11].
- US Department of State and other government branches and officials Dozens of other affected countries.
- The private sector (5 major newspapers: El País, Le Monde, The New York Times, The Guardian and Der Spiegel. And companies: namely Amazon, Paypal, MasterCard, Visa, Google, Twitter, Bank of America, Apple, and other smaller players [11]).
- Anonymous [11], a global hacker collective.

Actions

Wikileaks released thousands of classified or secret diplomatic cables of the United States' Department of State, creating international tensions throughout the world; the US government intervened to try to stop the leaks.

Affected Layers of the Internet

All layers: physical, logical, information and user.

Power Relationships

The U.S. Government is arguably the most powerful government in the world. However hard they tried to stop it [11], sensitive information was still released. Twitter and Google fought the release of information [11].

The above was in part due to the widespread support WikiLeaks received from open information activists or even less politically oriented people around the world [11]. This might not be the case for every "information openness" initiative.

Anonymous does not have evident political clout, nor does it have clear leaders. However they have managed to scramble media and government attention by bringing down sites hostile to WikiLeaks [11]. They have allegedly been searched and some of them arrested in connection with the attacks, in the U.S. and Europe [11].

Outcome

U.S. Secretary of State – or a member of her staff – had allegedly ordered spying on United Nations' Secretary General [11].

A Federal Court asks Twitter secretly to give in information about WikiLeaks related people [11]. Twitter asks the court to make the order public and then proceeds to inform their users of the request [11]. A similar procedure was used to seize Google email data [108].

To prevent being shut down by the U.S. Government (either by blocking via ISP, demanding the hosting company to cease doing so, or some other means) WikiLeaks

asked followers to download their data and set up *mirror sites* with over 1,000 people doing so [11]. Encrypted copies were also made available online "in case something happens to Assange or the site" [12].

Julian Assange was granted asylum by Ecuador, and is hosted by their embassy in London [83].

U.S. and other Western governments strongly disapprove the leak, claiming "it puts lives in danger" (Assange claims he had approached them asking for which information to redact out for that purpose) [11].

16. Edward Snowden leaks information on NSA classified mass surveillance programs - 2013

Actors Involved

- The NSA and other US security agencies.
- Edward Snowden, a former contractor of the Agency who is being sought after by the US and has been offered temporary asylum by Russia [85].
- Venezuela, Bolivia and other Latin American countries.
- Russia.

Actions

Edward Snowden revealed secret programs (most importantly Prism [87]) of the National Security Agency in the United States, dealing with data related to electronic communications.

Affected Layers of the Internet

Information and user.

Power Relationships

The reasons for spying on allies may be related to third countries and weapon deals, and also stopping corrupt practices such as bribery [84].

The concern about NSA surveillance on American citizens is not new, as shows this Congress [89] document requesting the President and the Attorney General to submit any records of NSA requesting information from phone companies without a warrant.

In Germany the news of the surveillance program have been particularly unwelcome – some claim this is due to bitter memories from the Stasi [90]. Furthermore, there were elections coming up, which could have lead German politicians to react in a tougher way than they "normally" would. A German Congressman has requested Snowden to be granted safe passage to be questioned regarding the US "espionage" programs [91].

The US has warned countries granting asylum to Snowden (most notably Venezuela) about a risk of "damaging its bilateral relations with the US." [25]

Bolivian President, Evo Morales, indicated that his country "is ready to give political

asylum to the people who expose spying activities" [28]. On his way back to Bolivia, his plane was denied passage over the airspace of Spain, France, Portugal and Italy, forcing the delegation to land in Vienna [28]. This led to harsh statements by several South American politicians, who suspected the move was initiated by the United States [28]. There was also condemnation by the O.A.S., U.N., and UNASUR. [28]

U.S. House of Representatives rejected a bill that would have limited NSA's phone surveillance capabilities [77].

Outcome
European diplomats are claiming invasion to privacy and may hold back on free-trade agreement talks with the U.S. [74].

"Germany's federal prosecutor's office has also opened inquiries into the NSA debacle, with a view to establishing whether German laws have been breached."[75] There are new statements by Snowden regarding the involvement of Germany's own government in the surveillance [76].

As [103] shows, fears of surveillance might be drawing business away from American web-related companies.

A recent poll by Quinnipiac University (cited by Business Insider) suggests the American public is now more concerned on the invasion of civil liberties in the name of terrorism [26].

The incident involving Bolivian President's plane, although the U.S. was not directly – at least not officially – involved, fed some South American leaders' claims on "American Imperialism" and even neo-colonialism, as UNASUR's Cochabamba declaration shows [29]. They have demanded explanations and formal apologies from Spain, France, Portugal and Italy [29].

As this article in the Washington Post shows [32], the Bolivian plane's event's timeline is highly disputed; there is even the possibility that the plane had to land for technical reasons, and not due to any denial of access to a country's airspace [32].

17. Hackers Intrude into New York Times – 2012-2013

Actors Involved
- Hackers, allegedly Chinese, codenamed APT12 [96].
- China.
- The New York Times.
- Mandiant, a cybersecurity firm.

Actions
A New York Times report on the wealth of Chinese Prime Minister's relatives [96] triggered a series of intrusions into the newspaper's website and data.

Affected Layers of the Internet
Physical, information and user.

Power Relationships
The New York Times is a major newspaper and website in the United States [97]. Attacks coincided with an investigation done by a New York Times journalist, exposing the alleged fortunes of Chinese prime minister Wen Jiabao's relatives [96]. In the report, the Times revealed that Wen's family "have controlled assets worth at least $2.7 billion."[100] The newspaper was threatened of "consequences" by the Chinese government [96].

The New York Times (quoting information from Mandiant, network provider AT&T, and the US Federal Bureau of Investigations) claims there is evidence linking these attacks to Chinese official institutions, including the military [96].

Given the timespan of the attacks, and the involvement of the group in attacks to several industries, the intruders have been qualified as an advanced persistent threat (APT) by Mandiant [99].

Outcome
The attackers did not steal New York Times's customer data, and although they managed to penetrate the computers of 53 employees, they focused on data regarding Wen's family's wealth report [96].

Despite the significant outreach of the attacks, The Times reported "security experts found no evidence that sensitive e-mails or files from the reporting of our articles about the Wen family were accessed" [96].

The attacks stopped initially in January 2013 after the APT12 group was exposed; the exposure itself might have triggered the malware updates [101].

PART II

Instruments and Tools Used in the Cases

In this section we take a closer look at the instruments and intrusions that have taken place in each case. This helps us develop a more detailed view of the operational features of this set of cyber conflicts.

Accordingly, Table 2 presents an overview of the tools and actions executed by the attackers or defendants for each of the cases presented; these describe the actions among the actors described in Part I, which led to the outcome included there.

Table 2. Tools and actions executed by the actors in the cyber conflicts

Case number, date, & name,	**Tools used and actions**
1. Cuckoo's Egg	Hess: Piggybacking, or accessing a network along with an authorized user (LBL) and known vulnerabilities in operating systems (particularly a "bug in the GNU-Emacs program") [2]. Stoll: A honeypot, a bogus piece of information seemingly relevant to the hacker used to keep him online and track him [2]. The "defense team" tracked the intruder's activity using port log printouts [2].
2. Morris Worm	Morris worm was initially Leaked from a different location (MIT) to cover its origin (Cornell) [4]. The worm overloaded computers (denial of service) because of running too many copies in the same host [4]. Morris's spread mechanism is described on [92]: "Morris identified four ways in which the worm could break into computers on the network: (1) through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer; (2) through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer; (3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and (4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform."
3. Dutch Hackers and British Hackers	The Dutch attackers used undisclosed "fairly unsophisticated methods." [13, p344]. The British attackers used a route through the

	US to connect to Korean targets (a nuclear institute) [13, p37].
4. Operation Solar Sunrise	Attackers (teenagers from California and Israel) used Known vulnerabilities in operative systems [79]. The profile of the attack is described in [79]: "(a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data." Attackers also made it look like the intrusion was coming from several countries in Europe and the Middle East [79].
5. Moonlight Maze	The hackers (Russian "cyber-spies" [68]) simply "plucked" the data, since it data was not encrypted or protected behind a firewall when it was sent to a printer [80]. DoD's defensive measures included centralizing the route –gateways– through which information travels for unclassified data, and asking for a Department-wide change of password [13, p50].
6. Electronic Disturbance Theater (EDT)	The attacker-developers made available html code and java applets (browser add-ins) that allowed people to reload a website in an infinite cycle [62]. With the right amount of users participating in the "sit-in", this would result in a Denial-Of-Service attack. This would come to be known as "FloodNet" [61][62]. The Pentagon and other US and Mexican authorities (the "hacktivists" were supporting the Zapatista movement [60]) would change their site to, when detecting a FloodNet attack, opening many browser windows, eventually leading the browser and the host computer to crash and stopping the attack at the source. [107]
7. ILOVEYOU and several other worms	In order to appear innocuous, ILOVEYOU included a *.txt* "extension" in the filename, making it appear as a simple text file [16]. The real extension (not shown by Microsoft Outlook at the time) was *.vbs* – an executable file [16]. It would then spread to *every* contact in the address book, hiding the malicious intent even further by using senders *known* to the receiver [14]. The worm created a copy of itself in media files in the computer, destroying the original files with extensions as *.jpg*, *.mp3* and several others (this was particularly damaging to media related companies [22]). It also directed the computer's browser to a specific website, in order to sniff login information (usernames and passwords). [18, p493] Another (possibly unintended) consequence of the virus was overflowing email servers, resulting in either Denial of Service due to the overload, or forcing the entity to shut down their email service

	altogether (see for example how it affected the British Parliament) [19].
8. "Patriotic Hackers" Attacks	Hackers attacking from Belgrade –allegedly Serbs and Russians [13, p50]– sent thousands of requests to NATO's website, effectively resulting in Denial of Service to legitimate users. In particular, they used ping (short for Packet Internet Groper) [27], which is a request used mainly to check the availability of a host (in our current concern a website). In this case, however, it was used with malicious intent. The attackers also targeted NATO's email server with a virus similar to Melissa (see previous case) [27]. At least one US-based hacktivist group attacked US official sites with anti-war propaganda [30]. In retaliation for US accidental strike on the Chinese embassy in Belgrade, Chinese hackers attacked American government webpages [13, p51]. The hackers managed to gain control of various sites, including the Department of Energy's website, and they claimed also gaining control of WhiteHouse.gov [30]. In the DOE case, they did so by modifying the file containing the administrators' username and password, which was stored in their Web Server [30]. This way, they could pass as the site's legitimate administrators and access its control panel. Dutch hackers attacked a Yugoslavian ISP to support the NATO side [30]. American President Bill Clinton ordered state-sponsored cyber attacks on Yugoslav President Milosevic's foreign bank accounts [35].
9. Chinese Cyber Espionage	Chinese hackers have reportedly used a wide range of tools to infiltrate foreign networks, ranging from capitalizing zero-day (previously unknown) vulnerabilities in third-party systems, to sending emails impersonating trusted senders, and many other less sophisticated approaches [13, p171]. When gaining control of the systems, the Chinese have reportedly been able to control peripherals, including cameras and microphones [93]. This has given them physical world espionage capabilities, besides the obvious sniffing of digital information. China is also believed to be scanning through US military computers [13, p166], presumably in order to seize its current state, development and advances.
10. Estonia receives cyber attacks	Spam attacks targeted senior Estonian political officials; the parliament's email server was shut down, as it became inoperable [13, p176]. Official Estonian sites received Distributed Denial of Service

	(DDoS) [44] attacks, affecting the traffic loads through Estonian networks and "resulting in malfunctions or non-availability of Internet services." [13, p177] Initially, this offensive was conducted in a fashion similar to the Electronic Disturbance Theater's (see case 6) attacks: by developing a script to load over and over the targeted site, making it available for download, and coordinating a time to use it. [13, p178-179] An Estonian newspaper, *Postimees Online* received DDoS, and "bots" posted politically oriented comments in its forums [13, p177]. The *Postimees Online* shut down foreign access to its site, limiting the possibility of further attacks but also its international outreach [13, p177]. Both private and public actors, coordinated by the Estonian CERT, responded initial attacks; the latter had the technical lead role [13, p178-180]. Subsequent attacks did not rely on human operators but on botnets ("network of robots"), or automated networks used to attack virtual targets. These comprised three types [13, p182]: • Internet Control Message Protocol (ICMP) flood, which uses either a deceptive broadcast pretending to originate from within the network, a sufficient number of ping requests to overflow the target's bandwidth, or less commonly the sending of a specific package which leads to the target system to crash [45]. • SYN flood, in which the attackers impersonate a valid address in the network and send a request to connect with the target host; the host then responds and opens a terminal (SYN-ACK), but the attacker doesn't send the last part of the connection request (ACK), resulting in the terminal being not available for legitimate connections [45]. If enough terminals are attacked in this way in certain amount of time, the host becomes unresponsive. • Generic traffic floods [13, p182], in which the attackers send enough page requests to saturate the host's bandwidth, therefore denying access to legitimate users. For example: "Government and bank websites that normally received 1,000 visits a day crashed after receiving upwards of 2,000 hits a second." [46] Botnets are generally harder to counter; effectively mitigating the attacks can be done by reconfiguring the hosts in order to increase the bandwidth available for legitimate users (e.g. blocking a range of IPs, or packets from outside the country), or by taking actions in the networks surrounding the host, although the latter may require collaboration from third-parties, including those in other countries [13, p183].

11. The Russo-Georgian War	DDoS attacks were used against the sites of the Georgian President, Parliament, Foreign Ministry, Interior Ministry, news agencies and banks, and incorporated SQL injections and cross-site scripting (XSS) [13, p197]: • An Structured Query Language (SQL) injection, usually implemented as a malware vector, is the input of code into a website's data input, in order to execute malicious commands [49]: "It is the vulnerability that results when you give an attacker the ability to influence the Structured Query Language (SQL) queries that an application passes to a back-end database. By being able to influence what is passed to the database, the attacker can leverage the syntax and capabilities of SQL itself, as well as the power and flexibility of supporting database functionality and operating system functionality available to the database" [50]. For instance, in a site's contact form, the attacker inputs a string of characters in order to manipulate the site's SQL database, instead of merely sending information. Due to the potential exposure of the site's core data (e.g. usernames and passwords), "SQL injection is one of the most devastating vulnerabilities to impact a business" [50]. • Cross-Site Scripting (XSS) steals the victim's browser cookies as a way to hijack its session [51]. Cookies consist on information stored by websites in the client's browser in order to identify a session [51]. Therefore, if the attacker can steal the cookies, it can impersonate a legitimate user. Georgia blocked Russian IPs, as most of the attacks were traced back to the Federation; this proved ineffective because the attackers were prepared for it and rerouted the traffic through third countries [13, p199-200]. The most effective measure by Georgia was to temporarily transfer its sites to hosts in the United States, Estonia and Poland [13, p199]. The attackers defaced several Georgian government sites and displayed pro-Russian propaganda [13, p196-198]. International forums were also flooded with comments supporting the Russian version of the facts [13, p196-198].
12. Agent.btz and operation Buckshot Yankee	A thumb drive was used as the tool to infect classified networks [13, p205]. The infected classified networks were not connected to the Internet, and terminals connected to the network cannot transmit information to the public Internet [13, p207]. In order to overrule this limitation, Agent.btz used a virus (SillyFDC) which spreads through connected devices and mapped drives, mainly using the Autorun feature of Windows [13, p207].

	The virus, however, tried to connect to the internet using a beacon to request further instructions [13, p208]. It was neutralized largely responding to that very request (from the DoD network) and sending the virus to sleep [13, p208].
13. Conficker Worm	Conficker exploited a Microsoft Windows buffer-overflow vulnerability, and created a botnet ("a network of robots") [58]; each infected terminal looked for new victims under reach, and for new ways to communicate under Peer-to-Peer (P2P) protocols with the coordination center and other infected terminals [58]. The worm used dynamic (web) domain generation to coordinate the infected terminals, in order to avoid counter measures, which attack botnet control point addresses [58]. Some of its versions reportedly propagated through removable media [59]. Creators or administrators of the malicious software updated it continuously to avoid detection and counter measures by security actors; as of April 2009 versions A through E were seen [58]. Some of its versions had the ability to kill anti-malware processes [113].
14. Stuxnet, Flame and Duqu (Olympic Games)	Stuxnet delivered itself using a zero-day (previously unknown) vulnerability, and included a digital certificate to impersonate legitimate software; it had several (spreading) vectors, including modifying Siemens Step 7 software, USB drives, Local Area Networks, and Windows vulnerabilities [13, p221]. The digital signature used by Stuxnet was renewed after Symantec discovered the virus and notified the initial issuer (Realtek) [13, p218]. Stuxnet spread on to over 100,000 hosts, but reportedly caused harm only to Iranian nuclear facilities [13, p218]. There, it would go on to operate the centrifuges, using drastic changes in speed to cause permanent damage [13, p218]. The virus was also designed to open and close valves, and to mask its actions by using pre-recorded normal operation indicators, thus fooling the system and the operators into thinking there was nothing unusual going on [13, p220-221]. Specifically, Stuxnet targeted offline (not connected to the Internet) industrial control systems known as SCADA, an acronym for Supervisory and Control and Data Acquisitions of Siemens, by changing the code on the programmable logic controllers (PLCs) to cause the malfunction and to cover it from the operators [13, p220]. The code was changed via the Field Peripheral Gateways (PG), because PLCs do not use Windows [13, p222] and thus the virus could not infect them directly.

	DDoS attacks were launched against industrial control systems mailing lists, in order to prevent the security information related to the virus from spreading. [13, p218] Flame and Duqu are reportedly viruses used to explore the Natanz facility, in a phase previous to Stuxnet deployment [13, p219-220]. Duqu is a "Remote Access Trojan", capable of recording intelligence information on industrial facilities [13, p219-220]. Flame, which was "twenty times" bigger (file size-wise) than Stuxnet, could operate peripherals and gather several different types of information on the host and its files [13, p219-220]. Both Duqu and Flame laid the ground for Stuxnet by tampering with the target host's security settings [13, p220]. Stuxnet manipulated the centrifuges by changing the "frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed." [57] Stuxnet's code targeted very specific systems (PLCs controlling a particular type of centrifuge used in Natanz), being harmless to any other system it infected [13, p222].
15. Wikileaks	Wikileaks publishes the cables in collaboration with selected newspapers [11]. A Senator Lieberman's (an independent) staff member allegedly threatens Amazon with an investigation, for which the company kicked WikiLeaks out (resulting in the site being temporarily down) [11]. Visa, MasterCard, Paypal and other smaller actors would follow banning WikiLeaks [11]. Anonymous uses Distributed Denial of Service Attacks on those companies' websites, bringing Visa and MasterCard's sites out for a day [11]. Senator Lieberman's website was attacked as well, as was the website of the Swedish counselor representing the women pressing sexual assault charges against Julian Assange [11].
16. Snowden's NSA leaks	NSA captures meta-data, or accessory data to the communications (e.g. the sender/receiver), on a massive number of targets, following national security directives [88].

	The Guardian (UK) and Der Spiegel (Germany) report that a number of EU and European State buildings in the US were targeted as well [86]. The NSA accessed private data stored by Yahoo, Gmail, Apple, Microsoft and other Internet giants [88]. This was done taking it directly from the Internet Service Providers [87], which made asking the platform operators (e.g. Facebook) to provide the information themselves a moot action. This made it unnecessary for the agency to even get Foreign Intelligence Surveillance Act (FISA) orders. Among other arguments, the leaked NSA slides claim "There were too many email accounts to be practical to seek Fisas for all." [88]
17. Hackers intrude into New York Times	The timespan of the attacks ranges from October 2012 to January 2013 [96], and there is evidence suggesting a new wave of attacks by the same groups on August 2013 [98]. The hackers intruded using spear-phishing, a method that involves emailing employees with malicious links, and installed remote access tools (RAT) [96]. They also routed through American universities and companies in order to disguise their identities [96]. The intruders used malware known as Aumlib and Ixeshe [101]. The second wave of attacks included updated versions of both threats [101]. In the Ixeshe case, attackers modified network traffic patterns to avoid being discovered [101]. The attackers managed to steal every employee password [96]. The New York Times hired Mandiant, after the newspaper and AT&T's efforts proved insufficient [96]. The Times went to replace infected computers, "blocked the compromised outside computers, removed every back door into its network, changed every employee password and wrapped additional security around its systems." [96]

We now highlight the key features of tools, methods of damage, or "weapons" used in each case. Table 3 proceeds along the same line as table 2, case by case.

Table 3. Summary of tools or method used

Case number and name	Tools or method used
1. Cuckoo's Egg	• Piggybacking [2] • A honeypot (defensive) [2]
2. Morris Worm	• Attacking from a different location [4] • Denial of service by overloading the target's processing capabilities [4] • A bug in an email application [92] • Finger demon: a "sniffer" of limited information in the target host [92] • Trusted hosts: using a computer's user privileges to access information in another computer [92] • A program that guesses passwords by repeatedly inputting strings in the password field [92]
3. Dutch Hackers and British Hackers	• "Fairly unsophisticated methods." [13, p344] • Routing through computers in third countries [13, p37]
4. Operation Solar Sunrise	• Known vulnerabilities in operative systems [79] • "Probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data." [79] • Routing through computers in third countries [79]
5. Moonlight Maze	• The data was unprotected and not encrypted, so it was simply "plucked" [80] • Changing the gateways for unclassified data (defensive) [13, p50] • Organization-wide change of passwords (defensive) [13, p50]
6. Electronic Disturbance Theater (EDT)	• Floodnet: html code and java applets to reload websites in an infinite cycle [62] • Distributed Denial Of Service (DDoS) [62] • "The DOD used a counter-hostile Java applet against FloodNet" [10], reloading browser windows in a cycle on the attacking host [107]
7. ILOVEYOU	• Including a fake .txt extension in the filename [16] • Sending email to all contacts in the target's address book [14] • Impersonating known senders [14] • Copying the worm into media files in the infected computer [22] • Directing the target to a website and sniffing log-in information [18,

	p493] • Denial of Service due to overload of email servers [19]
8. Patriotic Hackers	• Distributed Denial of Service by repeatedly pinging the target host [27] • A virus similar to Melissa over email [27] • Modifying the server file containing the administrators' username and password [30] • Impersonating legitimate users
9. Chinese Cyber Espionage	• A wide range of tools [13, p171] • Zero-day vulnerabilities [13, p171] • Vulnerabilities in third-party systems [13, p171] • Emails impersonating trusted contacts [13, p171] • Control of peripherals, such as cameras and microphones [93] • Scanning through the target's network. [13, p166]
10. Estonia receives cyber attacks	• Spam attacks [13, p176] • Distributed Denial of Service (DDoS) [44] • Scripts to load over and over the target's website [13, p178-179] • Comments posted by bots [13, p177] • Shutting down foreign access (defensive) [13, p177] • Internet Control Message Protocol (ICMP) [13, p182] • SYN flood [13, p182] • Generic traffic floods [13, p182] • Botnets
11. The Russo-Georgian War	• Distributed Denial of Service (DDos) [13, p197] • Structured Language Query (SQL) injections [13, p197] • Cross-Site Scripting (XSS) [13, p197] • Blocking IPs from a specific country (defensive) [13, p199-200] • Routing through third countries [13, p199-200] • Transfer affected hosts to other countries (defensive) [13, p199] • Posting propaganda in international forums [13, p196-198]
12. Agent.btz and operation Buckshot Yankee	• A thumb drive for initial infection [13, p205] • Spreading through connected devices and mapped drives using the Autorun feature of Windows [13, p207] • A beacon to request further instructions [13, p208] • Impersonating the virus's control center and sending instruction to neutralize it [13, p208]
13. Conficker	• Exploiting a Microsoft Windows buffer-overflow vulnerability [58] • Looking for new victims in the vicinity of the infected host [58]

	• Peer-to-Peer (P2P) protocols to communicate with the coordination center and other infected terminals [58] • Dynamic domain generation for coordination of infected hosts [58] • Attacking botnet control point addresses (defensive) [58] • Propagation through removable media [59] • Continuous update to avoid detection [58] • Killing anti-malware processes [113]
14. Stuxnet, Flame and Duqu	• Zero-day vulnerability [13, p221] • Digital signature [13, p221] • Modifying third party software [13, p221] • Propagation through removable media and local area networks [13, p221] • Operating hardware in ways it was not designed for in order to cause malfunction [13, p218] • Pre-recording normal operation indicators [13, p220-221] • Revoking the digital signature (defensive) [13, p218] • DDoS to cybersecurity-related companies [13, p218] • Remote Access Trojan [13, p219-220] • Tampering security settings [13, p220] • Targeting specific hardware [13, p220] • Using the target's hardware to infect other equipment [13, p222]
15. Wikileaks	• Publishing classified or secret information on newspapers [11] • Threatening online companies (defensive) [11] • Banning WikiLeaks from several online platforms [11] • Distributed Denial of Service [11] • Creating copies in many hosts globally [11]
16. Edward Snowden's NSA leaks	• Capturing meta-data on a massive number of targets [88] • Gathering intelligence from buildings [88], probably using microphones or cameras • Taking data directly from the Internet Service Providers [87]

17. Hackers Intrude into New York Times	• Spear-phishing: emailing employees with malicious links in order to install Remote Access Tools (RAT) [96]
	• Malware
	  o Aumlib
	  o A modified version of Ixeshe
	• Stealing employee passwords [96]
	• Replacing infected computers (defensive) [96]
	• Company-wide change of passwords (defensive) [96]
	• Removing backdoors into the network (defensive) [96]

Layers of the Internet affected by the attacks described in each of the cases are presented on Table 4. Our approach uses the "layered model of cyber-space" introduced by Choucri and Clark on [104], and included on Appendix 3.

Table 4. Layers of the Internet affected

Case number, date & name	Layer(s) of the Internet Affected
1. Cuckoo's Egg	• **Physical**. Hess accessed data stored on hardware at the target installation.
2. Morris Worm	• **Physical**. The worm overloaded the infected hosts resulting in disabled hardware [4]. • **Application**. Morris's spread mechanism used applications such as SEND MAIL [92].
3. Dutch Hackers and British Hackers	• **Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
4. Operation Solar Sunrise	• **Logical** and **Information**. The former due to the implantation of malware for espionage purposes, and the latter because of the espionage operation.
5. Moonlight Maze	• **Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
6. Electronic Disturbance Theater	• **Physical** and **logical**. Distributed Denial of Service (DDoS) attacks affect both the infrastructure (physical) and its ability to carry traffic (logical).
7. ILOVEYOU	• **Information**, **logical** and **physical**. The primary intent of the virus destroyed files (information), while the secondary DDoS resulted in an attack to both the physical (infrastructure) and logical (ability to carry traffic) layers.
8. Patriotic Hackers	• All layers: **physical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Altering data on hosts with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.

9. Chinese Cyber Espionage	• **Information**[2]. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
10. Estonia receives cyber attacks	• All layers: **physical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Posting data on hosts (websites) relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
11. The Russo-Georgian War	• All layers: **physical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Altering data on hosts (for defacement or otherwise) with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
12. Agent.btz and operation Buckshot Yankee	• **Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
13. Conficker	• **Physical**, **logical** and **information**. Conficker takes part of the computing capabilities of its victims, and transmits using removable media [59] resulting in an attack to the physical layer. It modifies the software of the host to prevent being detected (information), and spreads through the Internet (logical).
14. Stuxnet, Flame and Duqu	• All layers: **physical**, **logical**, **information** and **user**. DDoS (on third-parties) resulted in an attack to both the physical and logical layers. Stuxnet also caused malfunction of hardware (physical). Altering data on hosts (for avoiding detection or otherwise) with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
15. Wikileaks	• All layers: **physical**, **logical**, **information** and **user**. The main operation of WikiLeaks was public release of information. Anonymous targeted DDoS attacked the remaining layers. Defensive measures dealt with users,
16. Edward Snowden's NSA leaks	• **Information** and **user**. Snowden's actions were focused on releasing secret information, related to specific agencies in the United States and elsewhere (user).

[2] The attack on cybersitter might have involved other layers, but there isn't enough information available (from the sources reviewed for this paper) to assess it. In general, this case deals with extraction of information.

17. Hackers Intrude into New York Times	• **Physical**, **information** and **user**. Installing malware tools resulted in an attack to the physical layer. The episode was targeted, affecting the user layer. Accessing non-public information resulted in an attack to the information layer.

PART III

Inferences and Insights from the Individual cases

This section presents the author's own inferences and observation about key factors of relevance for each case, in the light of the information presented on previous sections. These are politically significant and distinctive "findings."

1. Cuckoo's Egg

Hess had trouble getting help from public officers even though this event happened during the Cold War and the KGB turned out to be involved.

2. Morris Worm

The media and the general public seem to have taken the Morris Worm as an indication of the Internet vulnerability. This must be looked considering the novelty of the Internet in 1989 and the extremely limited number of users it had when compared to the net nowadays.

A remarkable fact is the ability that an individual had to affect a large network, with access to relatively modest resources.

3. Dutch Hackers and British Hackers

It is possible that the intruders were planning to sell the information they collected.

4. Operation Solar Sunrise

Rather than being the exception, to this point in the timeline it looks as if teenagers or otherwise young hackers with a sense of grandiose goal are the rule in big cyber attacks.

5. Moonlight Maze

Arquilla's assertion (See Part II, case 5) seems sound, since the cases we have seen up to this point in time have been perpetrated mostly by non-radical, non-Al Qaeda-like affiliated people, but rather by lone wolves with non-war intentions.

What's unusual about Moonlight Maze is that after 15 years it remains highly classified, perhaps speaking about the seriousness of the incident.

One interesting fact regarding L0pht's (Boston-based hacking group) hearing on [36] is the lack of interest on foreign attacks, the same year Moonlight Maze happened – only a few questions addressed the subject in a one-hour testimony in Congress. A possible explanation for this is the lack of unclassified information there was (and still is) on the incident.

Policy makers wanted to address the issue of companies having no incentive to enhance security on [36] but appeared not to know how at the time this took place, resulting in a very cautious approach. The relatively specialized knowledge required to address issues of cybersecurity might be an impediment for policymaking in these issues.

Another highlight of [36] is that the hackers used pseudonyms on a public hearing, an event hardly imaginable in a domain different than cyberspace.

6. Electronic Disturbance Theater (EDT) attacks Pentagon

EDT's attacks, although apparently restricted to Mexican and US-immigration issues [62], have the potential to be replicated basically anytime, anywhere. Given the availability of tools provided by EDT (FloodNet), minimum technical skills would be required.

One consequence of Denial-Of-Service attacks is that users who may support the hacktivists' cause and need to use the attacked website are also affected. A possible analogy is a group of people blocking a highway (common in Venezuelan and other countries' street protests) and blocking passage to everybody, including their supporters. The obvious unintended consequence is the loss of supporters, although this might not be comparable to the impact on the media that such an event may have.

7. ILOVEYOU and several other worms released

The collective revenue of antivirus vendors increased 37% from 2000 to 2002 [20, calculation by the author], a fact consistent with heightened cyber security by private and public actors for the aforementioned period. Correlation with other variables has not been controlled, and causation can't be established; there might be other reasons for these increased sales (e.g. growth of the Internet itself).

Punishment for the perpetrators of Melissa (US) and ILOVEYOU (Philippines) only highlight how surreally different can the consequences of a similar crime be across different jurisdictions. This is the case, naturally, for other types of crimes, but it seems to be particularly significant in cyberspace.

8. "Patriotic Hackers" Attacks

While terrorism itself can be an act of war, our emphasis here is on the possible consequences of getting involved in an active international conflict as a *physical* terrorist or as a *cyber* terrorist. Any physical act of terror is presumably harder to cover and will probably be prosecuted in a tougher manner than an act of cyber terror. Furthermore, large-scale terrorist attacks (e.g. 9/11) may involve members of the terrorist groups doing the ultimate sacrifice, a suicidal operation. In cyber-based terrorism, this has hardly ever been the case. The risks and the consequences of cyber terrorism are thus much lower than that of physical terrorism. We can then assume this could be an incentive for terrorist groups to get involved in cyber-based attacks in the future.

Keeping the distances, the potential effect of a (deployed) petty officer's actions and a hacker are hardly comparable; the former takes a much higher risk – going all the way up to death – whilst the latter only faces (potentially) prosecution; and in the Chinese case, they are almost certain to walk. The point here is that cyberspace as a domain is giving previously non-existent or non-represented actors the possibility to actively participate in a major international conflict.

9. Chinese Cyber Espionage

If Cybersitter's allegations (See Part II, case 9) are true, one conclusion is that the Chinese government itself is involved or encourages cyber espionage for policy-related goals.

10. Estonia receives cyber attacks

The necessity for international cooperation [13, p184] in order to successfully counter cyber terrorism [46] was highlighted by these attacks.

The attacks probably did not achieve any of the goals described on II.10 (Outcome) for Russia because they were unsuccessful in significantly crippling Estonian ICT infrastructure, or operability, for a sustained period of time.

As Russia is economically and politically deterred to openly attack Estonia [46], a covert digital operation is certainly a viable alternative to exert international influence.

Accountability proved to be very different in the physical and cyber sides of this conflict (see II.10), both because of the difficulty of tracking the source of the cyber attacks, and the transnational nature of cyberspace.

It would be safe to assume that the industrial developed world, where the Internet and ICT infrastructures are generally better developed (as was the case in Estonia at the time of the attacks) would experience worse consequences following a cyber attack than developing nations.

The price for hiring a botnet ($75/day [13, p183]) highlights how resources can be enhanced in cyberspace: that much money wouldn't do much in traditional warfare. There, national budgets go up to U.S. $ hundreds of billions a year [52].

11. The Russo-Georgian War

Cyberspace proved once again to be a domain where accountability can be deflected. This attack also highlighted the potential to disrupt civilian systems in the cyber domain if there is a military might backing it up.

This case shows that the Kremlin can exert influence with tools in the cyber domain without necessarily dealing with the consequences of its actions in the international community. This is further shown by the fact that the cyber attacks continued even after the cease-fire was ordered [53].

Russian military superiority was also backed in the cyber domain, given how asymmetric were the capabilities to use cyber tools in a war situation.

12. Agent.btz infects US classified and unclassified networks, leading to operation Buckshot Yankee to counter it

The long period it took to remove the DoD ban on thumb drives may be related to the time it took to eradicate the threat in military networks, "more than one year"[54].

13. Conficker Worm

This case, which [58] reports as not the only one of its kind, highlights the possibility to build a profitable (and massive) network of computers for cybercrime.

The owners of the computers affected by Conficker may not know of the infection, presenting an accountability issue if the worm were to be used for more malicious goals.

14. Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic Games)

Source [57], besides arguing against the media hype surrounding Stuxnet, highlights the alleged willingness of governments, both in the West and elsewhere, to deal with criminal-originated tools in cyberspace.

The high profile of this operation is shown on the willingness to attack third parties (the industrial systems mailing list [13, p218]) in order to stop defensive efforts.

There are mixed reports regarding how long did Stuxnet delay Iranian procurement of a nuclear weapon. The Obama administration argued it pushed the development until at least 2015 [13, p230].

15. WikiLeaks

Julian Assange's final goals are unclear and may even be qualified as obscure – this led members of his team to leave WikiLeaks and form OpenLeaks under a "less authoritarian" structure [11]. He simultaneously claims he wants to change or remove "authoritarian conspiracies" (i.e. governments) [11] and plans to run for the Australian Senate [72]. WikiLeaks is a political party there already [72].

Whichever the original intentions for the leaks are, their effect on people's trust on democratically elected governments may be significant – and they are certainly used in the rhetoric by more authoritarian regimes such as Russia and China, as [73] shows for the latter.

Private companies, particularly large platforms such as Amazon, may have been more concerned about the consequences of continuing hosting WikiLeaks against the U.S. government's will (which could of course do harm to their business).

The major newspapers that joined in did so in the light of the information to be revealed (that's their business) but what's unusual here is their alliance with WikiLeaks. There are probably not many examples where cyber-only players have received the support of major mainstream media organizations.

US spying on UN's Secretary General generated outrage, in a way presumably similar to the current reactions to NSA surveillance of US allies. WikiLeaks is the only case in this study comparable to the NSA leaks, and the US government's reaction seems to have been quite similar – i.e. discrediting the source and trying to do damage control rather than to deal openly with the issue.

16. Edward Snowden leaks information on NSA classified mass surveillance programs

This case marks a major difference on how the government –and, given their relatively mild reaction, also the public– see cyberspace-based information collection as opposed to more physical seizes of information. If there were to be NSA agents peeking into people's homes (without actually getting in) the people's opposition might well be much stronger.

The incident involving Bolivian president's plane is likely harmful for American and European interests in the affected South American countries. It represents a reverberation of Snowden's revelations (basically delivered on the cyber domain) on the domain of international relations.

American officials seem to be trying to brush out and downsize the implications of NSA surveillance, both domestically and abroad.

The NSA's argument "it would be impractical to get FISAs for all" [88] is not hard to refute; if, for example, there were to be a lead to a terrorist in a neighborhood, would it be "impractical" to get warrants before accessing dozens of houses during the lookout? What would be the people's reaction to this? And finally, why would accessing someone's house be different from accessing phone or Internet content? Seriously addressing these questions in the future is cumbersome for both researchers and policymakers.

17. Hackers Intrude into New York Times

The New York Times is a big actor with significant political clout and widespread influence. Even as the Chinese government threatened them, they went ahead and published the controversial report on Wen's family wealth.

As Mandiant (basically a contractor of The Times in this case) exposed the group, they were forced to retrieve, albeit temporarily.

The above contrasts with attacks on Cybersitter (see case 9 on this paper, Chinese espionage), where the company, a much smaller player, exposed Chinese hacking but couldn't stop them from using its proprietary software.

The bigger and more powerful the actor, then, the more likely it will be able to deter Chinese intrusions or otherwise defend itself effectively.

PART IV

Conclusion: Some Critical Features

The cases presented in this paper are very diverse in their scope, actors, tools used and outcome. Table 5 introduces a broad categorization for the cases in espionage, malware, attack or warfare, and public release of secret government information.

Table 5. Broad classification of the cases

Case number and case	Category
1. Markus Hess hacks into several US military and research facilities (Cuckoo's Egg)	Espionage
2. Morris Worm	Malware
3. Dutch Hackers and British Hackers	Espionage
4. Operation Solar Sunrise	Espionage
5. Moonlight Maze	Espionage
6. Electronic Disturbance Theater (EDT) attacks Pentagon	Attack or warfare
7. ILOVEYOU and several other worms released	Malware
8. "Patriotic Hackers" Attacks	Attack or warfare
9. Chinese Cyber Espionage	Espionage
10. Estonia receives cyber attacks	Attack or warfare
11. The Russo-Georgian War and its cyber component	Attack or warfare
12. Agent.btz infects US classified and unclassified networks, leading to operation Buckshot Yankee to counter it	Malware
13. Conficker Worm began to spread	Malware
14. Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic Games)	Attack or warfare
15. Wikileaks releases thousands of diplomatic cables pertaining to the US State Department and its Missions abroad	Public release of secret government information
16. Edward Snowden leaks information about NSA classified mass surveillance programs	Public release of secret government information
17. Hackers Intrude into New York Times	Espionage

Some common conclusions can be drawn about the overall features of cyber conflicts. After extracting the conclusions, they were classified as related to (a) actors (b) socio-political context (c) tools and other technical issues (d) sophistication of the attacks (e) outcome and damage and (f) accountability, and are presented below.

(a) Actors

Cyberspace has brought in a number of new players to international conflict, and traditional actors (notably states) have increasingly –albeit slowly– recognized the importance of the domain.

- International cooperation, including both public and private actors, has proven indispensable for effective cyber defense when under attack.
- The involvement of the private sector on cyber defense has been critical in many cases. This is referred to in [13, p22] as "perhaps the biggest difference between cyber conflicts and their traditional equivalent…"
    - 16 out of the 17 cases studied involved the private sector either in attack or defense.
- On the State-sponsored side, the incidents present an increasing level of sophistication, extent and consequences.
- Private citizens, who otherwise probably wouldn't have a voice in international conflicts, have participated in conflicts on the cyber domain.
- Some countries, notably Russia and China [13, p204], have taken advantage of the previous point to recruit cyber volunteers for militia-like attacks.
- There is no evidence in the cases studied supporting that terrorist organizations have acted stand-alone on the cyber domain.

(b) Socio-Political Context

We are at the early stages of understanding the political implications of conflict in cyberspace. International agreements are unclear on the subject and a single country, the United States, still has significant power. The findings presented here are US-centered, as this paper was developed using such a focus. However, 23 countries are involved in at least one case, either in attack or defense. Countries involved in two or more cases are (frequency in parenthesis): United States (16), Russia (7), China (3), Israel (3), The Netherlands (2) and Germany (2). Six of the cases presented had a global reach. Also, given the importance of the US in cyberspace, this perspective shouldn't impose significant limitations on the conclusions to follow.

- All of the major international cyber conflicts presented here have been related to an ongoing conflict in the physical domain. This is consistent with [13, p21] "The more strategically significant a cyber conflict is, the more similar it is to conflicts on the land…"
- Awareness of the importance of conflicts in the cyber domain has steadily increased for policymakers, reflected on the outcomes of many of the incidents presented here.
- Rich industrialized countries with a highly developed ICT infrastructure are at a higher risk concerning cyber attacks.

- The target of the attacks varies significantly in the presented cases; they range from nuclear facilities, to military or classified networks, to random computers in order to create cyber criminal networks.
- Motivations for pursuing attacks on the cyber domain are also very dissimilar, ranging from political or social activism, to stealing intellectual property, to for-profit crime, to State-sponsored warfare.
- The general population's reaction to the NSA leaks and the WikiLeaks has been relatively mild; this may be related to intrinsic differences on people's views related to the cyber domain as opposed to the physical domain.

(c) Tools and other Technical Issues

The attacks studied in this paper have used significantly diverse tools, both on cyberspace and the physical world. This might be related to the sophistication of the actor, the amount of resources available, and the target of the hit.

- Distributed Denial of Service (DDoS) is by far the most common type of cyber attack. Others include SQL injection, Cross-Site Scripting (XSS), email-based malware, and identity theft or defacement.
- Air-gapped networks, or networks not connected to the public Internet, have not been exempt from attacks, as Stuxnet and Buckshot Yankee (Cases 12 and 14) show.
- The tools used by attackers vary wildly, and so do the measures to counter them:
    - Hackers have used email, known or unknown vulnerabilities in operating systems, deception, and outsourcing of traffic attacks, among other attack tools.
    - The measures to counter attacks include bringing down the affected hosts or disconnecting them from the Internet, counter-attacks, software patches, relocation of the servers in different countries, among others.

(d) Sophistication of the Attacks

- Sophistication varies greatly between cases; however, it seems like a perpetrator does not need highly specialized technical knowledge to intrude computer networks, a counter-intuitive fact.
- Sophistication of for-profit malware tools has been, nevertheless, steadily increasing, as is shown by Conficker (Case 13).
- Diverse layers of the Internet are affected for each case. The more sophisticated the attack, particularly if a State backs it, the more likely it is to affect all layers.

(e) Outcome and Damage

Some of the incidents presented here have had significant consequences on different dimensions. The Internet is now ubiquitous in developed countries, and there is little evidence suggesting it will not continue on expanding; this will probably further increase the potential damage of a cyber strike.

- The economic impact or cost of cyber conflicts is hard to estimate. One factor feeding that is the general unwillingness of both private and public actors to

release such information.

- The NSA leaks and the WikiLeaks show that information secrecy is particularly difficult to maintain on the cyber domain.
- The United States has done a number of exercises on cybersecurity; the outcome of some of them remains highly classified, making it difficult to evaluate the actual risks present on the cyber domain.
- The size of the actor under attack could have an influence on its ability to deter the attackers with actions in the physical world.
- Only about a third of the cases (6 out of 17) have "global reach." Most of the attacks are restricted to either one or a handful of jurisdictions.

(f) Accountability

The Internet's architecture makes it difficult to tell where the information is originally coming from [36], making accountability difficult; when adding sophistication to an attack, it becomes cumbersome to hold the culprits responsible, particularly for powerful attackers.

- The entrance barriers (including the monetary cost) for any actor to get involved in a conflict seem to be lower in the cyber domain than in the physical domain.
- The previous point may be related to the more difficult attribution of accountability in the cyber domain, and the relatively less harsh consequences for the perpetrators of cyber crime.
- Accountability gets further obscured when the attacks transcend national borders (and jurisdictions), which is very often the case.
- Punishment for cyber crimes varies wildly across jurisdictions.
- Difficulty in effectively holding a nation accountable has probably been an incentive for countries such as Russia, China and the United States to use cyber-based warfare or espionage tools.
- Accountability has proven difficult for large-scale cases, making it a desirable tool for States willing to push their international agendas.
- Furthermore, direct attribution might not be an advisable goal for policymakers involved in cyber conflict: "Attribution, which usually starts at the most technical level before working up to the people and organizations responsible, usually is not a helpful approach for such strategically important cyber conflicts." [13, p265]

Closing Notes

The framework used in this study has proven valuable when analyzing cyber conflict in an internally consistent way, and could be used for further work. Future study in this field is needed in order to gauge lessons from a higher number of cases, perhaps including perspectives from countries other than the United States. Particular categories of Table 5 might be addressed individually in the future, since they might have more common features and yield a better picture of that specific type of conflict. Also, researchers should assess people's perception of cyberspace, particularly related to privacy; the mild reactions to NSA revelations and WikiLeaks may not be fully understood until such studies are conducted.

Significance of cyberspace as a domain for international relations will likely increase overtime, as reflected by recent (unsuccessful) ITU efforts to regulate the Internet. Literature on this subject is definitely in its infancy, presenting obvious challenges for policymaking. Scientific research on international cybersecurity is a continuous necessity, particularly for developed countries such as the United States, with higher stakes on the event of an attack. Further studies should aim at addressing both technical and policy issues, since there is an intrinsic feedback among them when dealing with the Internet and cyberspace.

There are five appendices to this paper:

1. A brief set of exercises related to cybersecurity in the United States.
2. The main matrix generated with the framework used in this study, containing the information of the 17 cases[3].
3. Choucri and Clark's model of the layers of the Internet.
4. A list of countries involved in each case.
5. Selected significant cyber incidents, which is the base list for future work by the same author.

[3] There might be minor differences in the contents of the appendix and the main body of this paper.

Appendices

Appendix 1. A brief set of US government's actions and reports related to cybersecurity.

Report or action and date	Actors involved	Tools used	Power relationships	Outcome, "lessons learned" and observations
11th February 1970 **US DEFENSE SCIENCE BOARD GROUP REPORT ON COMPUTER VULNERABILITY US** [69]	DoD and other military related agencies [1]			This may be one of the first formal recognitions of cyber vulnerabilities by the US government. Provides guidelines for protecting classified information and systems [1].
1995 - Airforce 609th Information Squadron Creation [69]	US Military	"The first operational information warfare (IW) combat unit in United States Military history" [7]		1.- The main highlight here is the formal creation of a unit devoted to prevent cyber attacks to the US military: "This is not an experiment, this is an operational combat unit capable of defending our networks," [78] 2.- "Unclassified [communication] is our primary concern. The classified networks are fairly secure (…) But you could still bring somebody to their knees if you take out their unclassified communications." [78] The inclusion of more functions into cyberspace, which would potentially use unclassified networks, is likely to bring more vulnerability and the need for stronger security and more supervision of the networks.

Operation ELIGIBLE RECEIVER, 1997	The NSA acting as the red team, simulating an enemy intrusion [13, p42] The DoD as the target of such attacks [13, p42]	The NSA intruders used tools "readily available in the internet" to gain access to DoD systems. A dummy file was created in the folders to which they accessed [13, p42].	This was an internal exercise, but given the ease with which the simulated attacks were made, it draw substantial attention from top US officials [13, p345].	The lessons learned were shared with NATO partners [13, p40], reflecting both an increased concern for military cybersecurity and a will to enhance international cooperation in the matter.

Appendix 2. Matrix summarizing the cases.[4]

Case number, Case and date	Actors involved	Tools used and actions	Power relationships	Outcome	Inferences and Observations
1. August 1985 Markus Hess hacks into several US military and research facilities (Cuckoo's Egg)	• Markus Hess / German citizen working for KGB [2][64] • Clifford Stoll / Systems Administrator for Berkeley Lab [2][64]	Hess: Piggybacking, or accessing a network along with an authorized user (LBL) [2] Stoll: A honeypot, a bogus piece of information seemingly relevant to the hacker used to keep him online and track him [2].	Stoll had difficulties attracting attention to the case from officials, since they were "more concerned with 'real' crime and counterintelligence than the hard-to-fathom world of networks" [13, p7]	Hess and associates obtained "sensitive semiconductor, satellite, space, and aircraft technologies." [3]	Hess had trouble getting help from public officers even though this event happened during the Cold War and the KGB turned out to be involved.
2. November 1988 Morris Worm	Robert Tappan Morris [5] Cornell University [5]	Leaked from a different location (MIT) to cover its origin (Cornell) [4]. The worm overloaded computers (denial of service) because of running too many copies in the same host. [4] Morris spread mechanism is described on [92]: "Morris identified four ways in which the worm could break into computers on the network: (1) through a "hole" or "bug" (an	This was most likely a one-man-act and was duly condemned by the Cornell commission who investigated the case: "This was not a simple act of trespass analogous to wandering through someone's unlocked house without permission but with no intent to cause damage. A more apt analogy would be the driving of a golf cart on a rainy day through most houses in a neighborhood. The driver may have	A relatively large fraction of the computers connected to the Internet at the time were infected (some quote 10% [70]). The Cornell commission investigating the case fended off attempts to portray Morris' actions as heroic: "Although such security flaws may not be known to the public at large, their existence is accepted by those who make use of UNIX." [5] Morris was sentenced to 3 years	The media and the general public seem to have taken it as an indication of the internet vulnerability. This must be looked considering the novelty of the internet in 1989 and the extremely limited number of users it had when compared to the net nowadays. Something remarkable is the ability that an individual had to affect a large network, with access to relatively modest resources.

[4] For the most updated information, see the main body of this paper.

		error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer; (2) through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer; (3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and (4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform."	navigated carefully and broken no china, but it should have been obvious to the driver that the mud on the tires would soil the carpets and that the owners would later have to clean up the mess." [5]	probation, 400 hours of community service and fined $10,000 [79]. The DoD funded the creation of the first-ever CERT at Carnegie Mellon University. [13 p32]	
3. 1990-1991 Dutch Hackers and 1994 British Hackers	Unnamed Dutch "teenage hackers" [6]. US Military North and South Korean installations. [13, p37]	The Dutch attackers used undisclosed "fairly unsophisticated methods." [13, p344]. The "(teenagers from Holland) intruded into the networks of 34 US military installations during the lead up to the first Gulf War. Using fairly unsophisticated methods, the hackers were searching for information on missiles,	USDA website [6] states that no foreign intelligence agency was proven to be involved.	The US military didn't know for hours if the target was in North or South Korea, and if it were to be the former it could have been interpreted as a threat by the regime, at the time in negotiation with the US regarding their nuclear program [13, p37]. The target was, however, in South Korea [13, p37].	It is possible that the intruders were planning to sell the information they collected.

		nuclear weapons, and DESERT SHIELD." [55] The hackers from the Netherlands gathered information for "over a year" regarding US operations prior to the Gulf War. [6] The British attackers used a route through the US to connect to Korean targets (a nuclear institute). [13, p37]			
4. Operation Solar Sunrise, Feb 1998	Two teenagers from California and one teenager from Israel (Tenenbaum) [65]. Military agencies in the US and Israel	Attackers used Known vulnerabilities in operative systems [79]. The profile of the attack is described in [79]: "(a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data." Attackers also made it look like the intrusion was coming from several countries in Europe and the Middle East [79].	This attack had apparent massive mobilization due to the suspicion of 'Iraqi warfare' and went all the way up to the US President's Office [9]. "Although all DoD targeted systems were reported as unclassified, many key support systems reside on unclassified networks (Global Transportation System, Defense Finance System, medical, personnel, logistics, and official e-mail)" [67] Tenenbaum, the Israeli teenager, claims his objective was to "show the systems' vulnerability" rather than to cause harm [9].	This real world incident led to the creation of the Joint Task Force for Computer Network Defense (JTF-CND) by the US Department of Defense [13, p44-47]. For the first time there was a centralized unit capable of (and responsible for) responding to cyber attacks "crossing borders between commands and agencies" [13, p44-47]. The JTF-CND would initially report directly to the Secretary of Defense, although it was moved under the US Space Command within a year [13, p44-47]. An interesting feature of the JTF-CND was the coordination with the private sector in "critical industries" via the National Infrastructure Protection Center (NIPC) [13,	Rather than being the exception, to this point in the timeline it looks as if teenagers or otherwise young hackers with a sense of grandiose goal are the rule in big cyber attacks.

			Tanenbaum was later convicted for credit card fraud [66]. The US had ongoing tensions with Iraq at the time related to weapons of mass destruction [104]. US suspected the attacks came from Iraq, but found the Californian teenagers instead. [13, p43] [9]	p44-47]. JTF-CND's mission was expanded to potentially include Offense, renaming it to JTF-CNO, with the last "O" standing for Operations [13, p44-47]. The outcome of the attack was consistent with the findings of operation Eligible Receiver (see Appendix 1): "DoD has no effective indications and warning system, intrusion detection systems are insufficient, DoD is not organized effectively for IO, and that identifying the threat group and motives is a problem." [79]	
5. Moonlight Maze (Russians attack US Military and universities), March 1998	"Russian cyber-spies" targeting US Military, agencies and "leading civilian universities" [68] "Corrective" actions coordinated by National Infrastructure Protection Center (NIPC) and Joint Task Force for Computer Network Defense (JTF-CND) [69]	The hackers simply "plucked" the data, since it data was not encrypted or protected behind a firewall when it was sent to a printer [80]. DoD's defensive measures included centralizing the route –gateways– through which information travels for unclassified data, and asking for a Department-wide change of password. [13, p50]	Details remain classified, but according to a professor in the area the attacks were traced back to Russia, although he admits that this is no indication of the source of the attack [81]. This turned out to be a high profile case resulting in a "wake-up call to the DoD". In DoD's words "Defense exercises and real world events in 1997 and in early 1998 demonstrated the need for an organization within the Department to coordinate its defensive	John Arquilla, a professor of defense analysis, says regarding this incident "In the realm of cyberspace-based disruptive threats, we haven't yet had what they call the electronic Pearl Harbor" [70]. "What we really are talking about is a social gulf between those who have the skills to do costly disruption and those who are radical enough to want to do it." [70] The same year this happened a group of hackers testified in front of the Governmental Affairs Committee of the US Senate [36].	Arquilla's assertion (left cell) seems sound, since the cases we have seen up to this point in time have been perpetrated mostly by non-radical, non-Al Qaeda-like affiliated people, but rather by lone wolves with non-war intentions. One interesting fact regarding L0pht's hearing on [36] is the lack of interest on foreign attacks, the same year Moonlight Maze happened – only a few questions addressed the subject in a one-hour testimony. A possible explanation for this is the lack of unclassified

			activities and to have the authority to direct the necessary actions for that defense."[82] The Secretary of Defense called this a "state sponsored attack" [13, p49]. At the very least, it showed the potential impact of a specialized, potentially state-backed, attack – as opposed to a random attack by some individuals with rather unclear goals.	An interesting conclusion of the hearing on [36], however, is that there were not many incentives for software companies to increase security in their systems. According to the testimony, "companies want to ignore problems… it's cheaper for them." The hackers also emphasized the difficulty of establishing where or from whom a particular action is coming from on the internet [36], a fact consistent with Moonlight Maze outcome. Shortly after Moonlight Maze, PDD-63 "sets a goal of a reliable, interconnected, and secure information infrastructure by the year 2003." [81] Also, "The National Infrastructure Protection Center (NIPC) was established as a result of PDD-63" [81]. The DoD's Joint Task Force for Computer Network Defense came operational that same year [13, p48].	information there was (and still is) on the incident. Policy makers wanted to address the issue of companies having no incentive to enhance security on [36] but appeared not to know how at the time this took place, resulting in a very cautious approach. Another highlight of [36] is that the hackers used pseudonyms on a public hearing, an event hardly imaginable in a domain different than cyberspace. What's unusual about Moonlight Maze is that after 15 years it remains highly classified, perhaps speaking about the seriousness of the incident.
6. Electronic Disturbance Theater (EDT) attacks Pentagon – September 1998	Electronic Disturbance Theater – a group of activists [63] on the cyber domain. The United States	The attacker-developers made available html code and java applets (browser add-ins) that allowed people to reload a website in an infinite cycle [10]. With the right amount of users participating in the "sit-in", this would result in a	In their website, they claim to be "engaged in developing the theory and practice of Electronic Civil Disobedience (ECD)." [63] Ricardo Dominguez, an associate professor at the	The socio-political nature of this attack is consequent with "Dorothy E. Denning's testimony before the U.S. House of Representatives: 'Both EDT and the Electrohippies view their operations as acts of civil disobedience analogous to street	EDT's attacks, although apparently restricted to Mexican and US-immigration issues [62], have the potential to be replicated basically anytime, anywhere. Given the availability of tools provided by EDT (FloodNet), minimum technical

	and Mexico	Denial-Of-Service attack. This would become to be known as "FloodNet" [10][61]. The Pentagon and other US and Mexican authorities (the "hacktivists" were supporting the Zapatista movement [60]) would change their site to, when detecting a FloodNet attack, opening many browser windows eventually leading the browser and the host computer to crash – stopping the attack at the source. [10]	University of California San Diego [62], led the EDT.	protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction'" [71] "While maintaining a focus on the Zapatista movement--paradoxically, a nomadic site-specificity-- EDT has realized the (potential) links between bottom-up struggles for social justice." [71]	skills are required. One consequence of Denial-Of-Service attacks is that users who may support the hacktivists' cause and need to use the attacked website are also affected. A possible analogy is a group of people blocking a highway (common in Venezuelan exhibitions) and blocking passage to everybody, including their supporters. The obvious unintended consequence is the loss of supporters, although this might not be comparable to the impact on the media that such an event may have.
7. ILOVEYOU and several other worms released, ca. 2000 [13, p50]	ILOVEYOU was developed in the Philippines by, among others, a former computer science student, Onel de Guzman. [14] [15] Philippines's National Bureau of Investigation (NBI), with the assistance of the US FBI [15] Microsoft, the	In order to appear innocuous, ILOVEYOU included a *.txt* "extension" in the filename, making it appear as a simple text file [16]. The real extension (not shown by Microsoft Outlook at the time) was *.vbs* – an executable file [16]. It would then spread to every contact in the address book, hiding the malicious intent even further by using senders *known* to the receiver. [14] The worm created a copy of itself in media files in the computer, destroying the	ILOVEYOU affected tens of millions of computers worldwide and had an estimated clean-up cost of USD 15 billion. [17] Despite this dramatic impact, the charges against the suspects were dropped: there was no law in the Philippines at the time punishing the development of malware [17]. There was no international treaty that would enable the prosecution of de Guzman. The ILOVEYOU episode	This worm was, given its massive reach, a wake-up call to a number of actors, including technology giants such as Microsoft [23]: "ILoveYou grabbed the entire world, for the first time, by the collar and forced it to take security seriously" [16]. The author –or one of them– of Melissa (an American citizen), a virus which spread about a year earlier than ILOVEYOU, was sentenced to 20 months in prison, fined USD 5,000 and ordered to "not be involved with computer networks, the Internet	The collective revenue of antivirus vendors increased 37% from 2000 to 2002 [20, calculation by the authors], a fact consistent with heightened cyber security by private and public actors for the aforementioned period. Correlation does not imply causation here, so there might be other reasons for these increased sales (e.g. growth of the Internet itself). Punishment for the perpetrators of Melissa (US) and ILOVEYOU (Philippines) only highlight how surreally different

	proprietary owner of the software through which the virus spread, the Outlook email client [23]. This worm affected a large number of private actors. According to McAffee, then the largest antivirus vendor, the worm infected "60 to 80 percent of its Fortune 100 clients." [22]	original files with extensions as *.jpg*, *.mp3* and several others (this was particularly damaging to media related companies [22]). It also directed the computer's browser to a specific website, in order to sniff login information (usernames and passwords). [18, p493] Another (possibly unintended) consequence of the virus was overflowing email servers, resulting in either Denial of Service due to the overload, or forcing the entity to shut down their email service altogether (see for example how it affected the British Parliament). [19]	increased awareness on the need to coordinate internationally – given the nature of cyberspace, i.e. transcending "constraints of geography and physical location"[24, p3]. See [18] for a review of some of the international initiatives under way in 2002, including actions by the European Union and G-8. Onel de Guzman left school his department rejected his thesis [15]. His work consisted in a proposal to massively steal passwords, in order to allow more people to connect to the internet [15].	or Internet bulletin boards unless authorized by the Court" [21]. By comparison, one of the authors of ILOVEYOU, causing much more widespread damage than Melissa (which limited itself to the first 50 contacts in the address book [22]), could not be sentenced in the Philippines. Instead he was free to be interviewed and brag about how he had "become part of the history of the Philippines."[14] This worm affected a large number of private actors. According to McAffee, then the largest antivirus vendor, the worm infected "60 to 80 percent of its Fortune 100 clients." [22]	can the consequences of a similar crime be across different jurisdictions. This is the case, naturally, for other types of crimes, but it seems to be particularly significant in cyberspace.
8. 1999-2001 "Patriotic Hackers" Attacks [13, p50]	The United States and its NATO allies Serb and Russian hackers American hackers Dutch hackers Chinese hackers China	Hackers attacking from Belgrade –allegedly Serbs and Russians [13, p50]– sent thousands of requests to NATO website, effectively resulting in Denial of Service to legitimate users. In particular, they used ping (short for Packet Internet Groper) [27], which is a request used mainly to check the availability of a host (in our current concern a website). In this case, however, it was used with malicious intent.	These attacks are perhaps the first instance where the episode can be called a cyberwar [30], because they were connected to the ongoing physical war in Kosovo. The US and Chinese responses to the cyber attacks originating from its territory were distinctly different. The former made it clear to its citizens that it did not encourage patriotic	One main consequence of this series of episodes is the emergence of cyber as a domain for warfare. Although [13, p27-40] shows that the consideration of cyber defense since at least two decades before 1999, the potential consequences should Kosovo related attacks been more successful "could have been devastating"[35]; this in turn showed the world, and military powers in particular, that "the Internet is no longer just a side issue." [27]	While terrorism itself can be an act of war, our emphasis here is on the possible consequences of getting involved in an active international conflict as a *physical* terrorist or as a *cyber* terrorist. Any physical act of terror is presumably harder to cover and will probably be prosecuted in a tougher manner than an act of cyber terror. Furthermore, large-scale terrorist attacks (e.g. 9/11) may involve members of the terrorist groups doing the ultimate sacrifice, a

		The attackers also targeted NATOs email server with a virus similar to Melissa (see previous case) [27]. At least one US-based hacktivist group attacked US official sites with anti-war propaganda [30]. In retaliation for US accidental strike on the Chinese embassy in Belgrade, Chinese hackers attacked American government webpages [13, p51]. The hackers managed to gain control of various sites, including the Department of Energy website, and they claimed also gaining control of WhiteHouse.gov [30]. In the DOE case, they did so by modifying the file containing the administrator's usernames and password, which was stored in their Web Server [30]. This way, they could pass as the site's legitimate administrators and access its control panel. Dutch hackers attacked a Yugoslavian ISP to support the NATO side [30]. American President Bill Clinton ordered state-sponsored cyber attacks on Yugoslav President Milosevic's foreign	hacking, given that "such activity is illegal and punishable as a felony." China, on the other hand, did little to encourage its own hackers to stop [13, p51]. This is consistent with dissimilar views of the internet as a tool for foreign policy [13, p50]. At the very least, cyber attacks on foreign targets were seen very differently in the two countries. At least some of the hackers here were regular citizens, presumably not involved in politics, the military or espionage, and with very limited actual political or military power. Cyberspace provided them with a venue to be actors in the war, with limited risks and a very visible outcome.	[35] Quotes that most of the attacks concerned in this case have been classified as cyber terrorism. The official response of the US was to shut down the DOE website until clarifying how the hackers managed to gain access [30]. The White House also closed its site for a few days largely as a preventative measure following hijacking attempts [30].	suicidal operation. In cyber-based terrorism, this has hardly ever been the case. The risks and the consequences of cyber terrorism are thus much lower than that of physical terrorism. We can then assume this could be an incentive for terrorist groups to get involved in cyber-based attacks in the future. Keeping the distances, the potential effect of a petty officer's (involved in the war) actions and a hacker are hardly comparable; the former takes a much higher risk – going all the way up to death – whilst the latter only faces (potentially) prosecution; and in the Chinese case, they are almost certain to walk. The point here is that cyberspace as a domain is giving previously non-existent actors the possibility to actively participate in a major international conflict.

		bank accounts [35].			
9. Chinese Cyber Espionage, 2005-2012* [13, p165-173] *These dates mark the first public US recognition of the Chinese intrusions and the latest time for which this case's sources address the issue; this is believed to be an ongoing threat [13, p173].	China. Agencies include "the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Second Department of the People's Liberation Army General Staff Department (2PLA), or the Liaison Office of the General Political Department." [42] Hacker groups based in China The United States, its allies, and over a hundred countries as the targets of the attacks [13, p167] Private firms in diverse economic sectors, mostly in technology	Chinese hackers have reportedly used a wide range of tools to infiltrate foreign networks, ranging from capitalizing zero-day (previously unknown) vulnerabilities in third-party systems, to sending emails impersonating trusted senders, and many other less sophisticated approaches [13, p171]. When gaining control of the systems, the Chinese have reportedly been able to control peripherals, including cameras and microphones [93]. This has given them physical world espionage capabilities, besides the obvious sniffing of digital information. China is also believed to be scanning through US military computers [13, p166], presumably in order to seize its current state, development and advances.	The head of the US National Security Agency and Cyber Command has estimated the loss for American companies in intellectual properties at USD 250 billion [13, p173]. This is, evidently, an enormous incentive to denounce and try to stop the Chinese espionage. That, however, has not been the case, with few exceptions such as Google denouncing what has been called "operation Aurora" [94]. There may be a number of reasons for the above. In the private actors case, denouncing China could lead to Beijing making it harder for them to do business there [13, p173]. Considering rapid Chinese economic expansion, and the fact that the middle class there is larger than the entire population of the United States [37], this is arguably a strong incentive not to publicly denounce Chinese intrusions.	There might be other reasons for companies not defying China publicly: although the intellectual property fight seems to be rising in the United States [40], fighting that fight in China may be more difficult; besides the inherently different Chinese framework for intellectual property [41], there might be little gain in trying to prosecute a Chinese hacker and recover the loss, since any enforcement would require diplomatic efforts [33]. There is a distinction to be made on what is generally qualified as "Chinese espionage."[42] The "conventional view" for Western analysts tends to categorize most types of espionage as if being State-sponsored [42]. In reality, the main goal of Chinese "official" intelligence is to protect the power of the Communist Party [42]. The highlight is that non-state actors also execute economic espionage, with or without official Chinese support or encouragement [42]. The Cox Report, the result of a US House of Representatives	If Cybersitter's (left cell) allegations are true, one conclusion is that the Chinese government itself is involved or encourages cyber espionage for policy-related goals.

			The US and China, as the world's two biggest economies [38], are also economically interdependent. Only in US Treasury Bonds, China is reported to own USD 1.25 trillion [39]. This, and the need for cooperation in geopolitical issues such as Syria and Iran [13, p173], may complicate US government public attempts at denouncing Chinese cyber espionage. APT1, a Chinese hacking group, has major infrastructure including "1,000 servers" and a "special fiber optic network" [99]. Unconventional agents include ethnic Chinese not physically present in China [42]. However, there seems to be a bias toward believing this to be the majority, while in reality that might not be the rule but rather an exception targeting dissidents or Taiwan [42].	commission, concluded that China had gained access to "advanced US thermonuclear weapons."[43] See the case where a small California-based company (Cybersitter) claims its software was basically stolen by the Chinese government for use in the Green Dam Project, the massive firewall preventing millions of Chinese users to access contents ranging from pornographic sites to politically oriented portals [33]. The company states the Chinese government owes it USD 2.2 billion [33]. The suit, however, had limited chance of success because it was done in a US court, with the alleged criminal activities happening in China [33]. Following the suit, the company received a cyber attack, presumably from China [34]. The Chinese hacking group identified by Mandiant (a cybersecurity firm) as APT1, is involved in economic espionage, attacking companies in many industries, and stealing commercial information [98][99].	

10. Estonia receives cyber attacks from April 17th to May 18th, 2007 [13, p174]	Estonia Russia Estonian private actors, including newspapers, technical associations, banks and individuals Public and private actors from NATO allies, particularly Finland, Israel, Germany and Slovenia [13, p184] [46] Russian and Russian-Estonian hackers, and members of the Russian diaspora worldwide, possibly supported by the Kremlin	Spam attacks targeted senior Estonian political officials; the parliament's email server was shut down, as it became inoperable [13, p176]. Official Estonian sites received Distributed Denial of Service (DDoS) [44] attacks, affecting the traffic loads through Estonian networks and "resulting in malfunctions or non-availability of Internet services." [13, p177] Initially, this offensive was conducted in a fashion similar to the Electronic Disturbance Theater's attacks: by developing a script to load over and over the targeted site, making it available for download, and coordinating a time to use it. [13, p178-179] An Estonian newspaper, *Postimees Online* received DDoS, and "bots" posted politically oriented comments in its forums [13, p177]. The *Postimees Online* shut down foreign access to its site, limiting the possibility of further attacks but also its international outreach [13, p177]. Both private and public actors,	The motivation for the attacks can be traced perhaps to earlier in 2007, when Estonia had announced it would move a WWII monument (the Bronze Soldier [48]) from the center of its capital Tallinn to a cemetery in the outer edge of the city [13, p174-176]. The monument carried strong symbolism for ethnic Russians living in Estonia and Russians alike, as it represented the Soviet victory over Nazi Germany (Russian decision-makers asked Estonia not to move the monument) [13, p174-176]. For some other Estonians, however, the monument was a symbol of Russian oppression during the USSR regime [13, p174-176] (Estonia became independent only six years earlier in 1991) [56]. As Estonia qualified the attacks as being of Russian origin, International cooperation, including several European countries	Estonia became a cybersecurity hub in the aftermath of the attack, as shows the "hosting of the NATO Cooperative Cyber Defense Center of Excellence and EU Agency for large-scale IT systems." [13, p187] The price of hiring a botnet with sufficient bandwidth to perform the attacks was $75/day [13, p183]. The suspicions of Russia being involved directly are not irrational. Former Soviet states, such as Estonia, are of particular importance in Russian foreign policy, and diminishing Western influence [13, p191] in the region is a very likely goal of the Kremlin. The volume of the attacks, and their coordination over time, also make Russia a viable suspect over an ad-hoc network of hackers in the Russian diaspora [13, p188-189] [46]. The use "of globally dispersed and virtually unattributable botnets"[46], and particularly those including computers used without the owner's knowledge (as was the case in Estonia) [47], obviously makes prosecution of	The necessity for international cooperation [13, p184] in order to successfully counter cyber terrorism [46] was highlighted by these attacks. The attacks probably did not achieve any of the goals described on the left cell (third paragraph) for Russia because they were unsuccessful in significantly crippling Estonian ICT infrastructure, or operability, for a sustained period of time. As Russia is economically and politically deterred to openly attack Estonia [46], a covert digital operation is certainly a viable alternative to exert international influence. Accountability proved to be very different in the physical and cyber sides of this conflict (see left cell – fifth paragraph), both because of the difficulty of tracking the source of the cyber attacks, and the transnational nature of cyberspace. It would be safe to assume that the industrial developed world, where the Internet and ICT infrastructures are generally better developed (as was the case

		coordinated by the Estonian CERT, responded initial attacks. The latter had the technical lead role. [13, p178-180] Subsequent attacks did not rely on human operators but on botnets ("network of robots"), or automated networks used to attack virtual targets. These comprised three types [13, p182]: • Internet Control Message Protocol (ICMP) flood, which uses either a deceptive broadcast pretending to originate from within the network, a sufficient number of ping requests to overflow the target's bandwidth, or less commonly the sending of a specific package which leads to the target system to crash [45]. • SYN flood, in which the attackers impersonate a valid address in the network and send a request to connect with the target host; the host then responds and opens a terminal (SYN-ACK), but the attacker doesn't send the last part of the connection request (ACK), resulting in the terminal being not	and Finland in particular, arose [13, p184-186]. This included individual foreign technical professionals, ISPs, network companies, and other private and public actors [13, p184-186]. The attacks were traced back to Russia, but the direct involvement of the Kremlin has not been proven [13, p189-190]. This did not stop, however, Estonian politicians and senior media officials of attacking Russian government directly in the aftermath of the attack, and the event "continues to frame Russian-Estonian relations today." [13, p188-189] The Estonian reaction may have been directed at discouraging future uses of cyber attacks to exert influence in international relations, particularly by Russia [13, p184-191]. Although for the context of this paper the cyber attacks are the central issue, the physical counterpart during	the culprits very difficult: "Estonian authorities made a few in-country arrests but never uncovered the main culprits, who were allegedly operating out of Russia" [46]. By contrast, 300 people had been arrested by the morning of the day after the street riots started [48].	in Estonia at the time of the attacks) would experience worse consequences following a cyber attack than developing nations. The price for hiring a botnet (see left cell, second paragraph) highlights how resources can be enhanced in cyberspace - that much money wouldn't do much in traditional warfare. There, national budgets go up to $ hundreds of billions over year [52].

		available for legitimate connections [45]. If enough terminals are attacked in this way in certain amount of time, the host becomes unresponsive [45]. • Generic traffic floods [13, p182], in which the attackers send enough page requests to consume the host's bandwidth, therefore denying access to legitimate users. For example: "Government and bank websites that normally received 1,000 visits a day crashed after receiving upwards of 2,000 hits a second." [46] Botnets are generally harder to counter; effectively mitigating the attacks can be done by reconfiguring the hosts in order to increase the bandwidth available for legitimate users (e.g. blocking a range of IPs, or packets from outside the country), or by taking actions in the networks surrounding the host, although the latter may require collaboration from third-parties, including those in other countries [13, p183].	the concerned period was present in the form of riots and street violence. [46] Even though the actual perpetrators of the DDoS attacks were also located outside Estonia (presumably members of the Russian diaspora [46]), these actions were a part of an ongoing clash among different ethnic populations (Russian and Estonian) in Estonia. Generally speaking, Estonia was an ideal target for a cyber attack because of its advanced ICT infrastructure and widespread Internet use: "97 percent of bank transactions occur online; and in 2007, 60 percent of the country's population used the Internet on a daily basis." [46]		
11. The Russo-Georgian	Russia Russian organized	DDoS attacks were used against the sites of the Georgian President, Parliament, Foreign	The cyber conflict offensive was simultaneous with the ongoing Russian operation	The most palpable impact on the general population was the downtime of the banks'	Cyberspace proved once again to be a domain where accountability can be deflected.

War 2008 [13, p194] – **and its cyber component**	crime Georgia Estonia and other NATO allies supporting Georgia	Ministry, Interior Ministry, news agencies and banks, and incorporated SQL injections and cross-site scripting (XSS) [13, p197]: • An Structured Query Language (SQL) injection, usually implemented as a malware vector, is the input of code into a website's data input, in order to execute malicious commands [49]: "It is the vulnerability that results when you give an attacker the ability to influence the Structured Query Language (SQL) queries that an application passes to a back-end database. By being able to influence what is passed to the database, the attacker can leverage the syntax and capabilities of SQL itself, as well as the power and flexibility of supporting database functionality and operating system functionality available to the database" [50]. Due to the potential exposure of the site's core data (e.g. usernames and passwords), "SQL injection is one of the most devastating vulnerabilities to impact a business"[50]. For instance,	on South Ossetia, a disputed region in the north of Georgia; South Ossetian independence efforts are openly supported by the Kremlin [13, p194-196]. The period leading to the war saw military exercises conducted by Moscow in South Ossetia and Abkhasia (another disputed region) [13, p194-196]. Conversely, Georgia made efforts to step up its military force and conducted exercises with NATO, although the latter's "troops had already left before the fighting with the Russians began." [13, p194-196] Although the direct involvement of Moscow was not (as in the attacks against Estonia) directly proven, "consider[ing] the forensic evidence, geopolitical situation, timing, and the relationship between the government, the youth, and criminal groups, it is not difficult to conclude that the Kremlin was behind it all"[13, p201]. This assertion is significant	electronic systems, denying people in Georgia access to their money [13, p198]. See also [53], which provides a case for the application of International Humanitarian Law to the Russo-Georgian cyber conflict. Appealing to nationalism, sites with a .ru [13, p201] (Russia) domain recruited, trained, and provided tools to new hackers in Russia and elsewhere. This has been called a cyber militia [13, p204]. It is in fact a Russian tactic goal to façade cyber attacks as of being of "criminal or terrorist" origin [13, p203]; similar cyber militia approaches have been taken by China and Iran [13, p204]. The outcome of the war itself has been described on [13, p196] as a "show of Russian superiority and the degradation of the long-term effectiveness of the Georgian military."	This attack highlighted the potential to disrupt civilian systems in the cyber domain if there is a military might potentially backing it up. This case shows that the Kremlin can exert influence with tools in the cyber domain without necessarily dealing with the consequences of its actions in the international community. This is further shown by the fact that the cyber attacks continued even after the cease-fire was ordered [53]. Russian military superiority was also backed in the cyber domain, given how asymmetric were the capabilities to use cyber tools in a war situation.

		in a site's contact form, the attacker inputs a string of characters in order to manipulate the site's SQL database, instead of merely sending information. • Cross-Site Scripting (XSS) steals the victim's browser cookies as a way to hijack its session [51]. Cookies consist on information stored by websites in the client's browser in order to identify a session [51]. Therefore, if the attacker can steal the cookies, it can then impersonate a legitimate user. Georgia blocked Russian IPs, as most of the attacks were traced back to the Federation; this proved ineffective because the attackers were prepared for it and rerouted the traffic through third countries. [13, p199-200] The most effective measure by Georgia was to temporarily transfer its sites to hosts in the United States, Estonia and Poland [13, p199]. The attackers defaced several Georgian government sites and displayed pro-Russian propaganda [13, p196-198].	when Russia is considered the second most powerful military power in the world [52]. There are indications of the participation of Russian criminal groups, which may be related to the Kremlin [13, p200-202]. Estonia supported Georgia, but the scope of the attacks meant that they mostly did damage control [13, p199].		

		International forums were flooded with comments supporting the Russian version of the facts. [13, p196-198]			
12. Agent.btz infects US classified and unclassified networks, leading to operation Buckshot Yankee to counter it, 2008 [13, p205]	The US Military NATO A "Russian foreign intelligence agency" (allegedly) [13, p206]	A thumb drive was used as the tool to infect classified networks [13, p205]. The infected classified networks were not connected to the Internet, and terminals connected to the network cannot transmit information to the public Internet [13, p207]. In order to overrule this limitation, Agent.btz used a virus (SillyFDC) which spreads through connected devices and mapped drives, mainly using the Autorun feature of Windows. [13, p207] The virus, however, tried to connect to the internet using a beacon to request further instructions, [13, p208]. It was neutralized largely responding to that very request (from the DoD network) and sending the virus to sleep. [13, p208]	Senior US Officials, including President George W. Bush and Secretary of Defense Robert M. Gates were briefed on the incident [13, p209], speaking of its gravity. The origin of the virus is uncertain; but "evidence suggests both that the US military is confident it knows who is responsible, and that it unofficially attributes a Russian foreign intelligence agency."[13, p207] There is no report in [13, p205-211] of the virus causing significant damage. This may have been either because the virus couldn't receive further instructions from its creator, or because it was intended for information gathering.	The incident led to a ban on thumb drives and other forms of removable media for over a year [13, p209]. This measure in itself is significant, since troops were reported to use such devices to transfer data when network resources are limited [13, p210]. According to [13, p210-211], Agent.btz and Buckshot Yankee changed the US Military in several different ways: • The NSA and the DoD began working together. In detecting and countering the virus, the NSA was a key player. • The creation of the Cyber Command, and the subsequent change in the cyber "culture, conduct and capability." • Cyber security was given a higher priority from this point forward.	The long period it took to remove the DoD ban on thumb drives may be related to the time it took to eradicate the threat in military networks, "more than one year"[54].
13. Conficker Worm began to spread in November	Cyber criminals, working for profit. (The exact origin remains	Conficker exploited a Microsoft Windows buffer-overflow vulnerability [58].	Botnets can serve several purposes, ranging from petty cyber crimes such as spam, to State sponsored	Conficker infected millions of computers [58], in 200 countries [59], causing $ millions in damage [58].	This case, which [58] reports as not the only one of its kind, highlights the possibility to build a profitable network of

2008 [58]	unknown, but evidence points toward Ukraine [102]) The Internet security community	A botnet ("a network of robots") was created with Conficker [58]; each infected terminal looked for new victims under reach, and for new ways to communicate under Peer-to-Peer (P2P) protocols with the coordination center and other infected terminals [58]. The worm used dynamic (web) domain generation to coordinate the infected terminals, in order to avoid counter measures, which attack botnet control point addresses [58]. Some of its versions reportedly propagated through removable media [59]. Creators or administrators of the malicious software updated it continuously to avoid detection and counter measures by security actors; as of April 2009 versions A through E were seen [58]. Some of its versions had the ability to kill anti-malware processes once per second [59].	warfare actions [58]. Evidence suggests Conficker was used "as a platform for conducting wide-scale fraud, spam, and general Internet misuse" for profit [58], rather than any State sponsored cyber warfare.	Some of the vulnerabilities were patched by the software vendors, but this can only help if the infected computers are patched, which is not the case for a "huge worldwide pool of poorly managed and unpatched Internet-ac- cessible computers." [58] The previous point highlights the need for a new security scheme of adaptation to dynamic (continuously adapting) security threats [58]. Whitehats, or hackers working on the cybersecurity side, created a new organization to deal with the widespread infection of Conficker, sharing technical knowledge and security insights with policymakers and the population at large [58].	computers for cybercrime. The owners of the computers affected by Conficker may not know of the infection, presenting an accountability issue if the worm were to be used for more malicious goals.
14. Stuxnet, Flame and Duqu cyber campaign against Iran (codenamed Olympic	The United States Iran Iranian nuclear facility in Natanz	Stuxnet delivered itself using a zero-day (previously unknown) vulnerability, and included a digital certificate to impersonate legitimate software; it had several vectors, including modifying Siemens	The initial purpose of Iranian nuclear program was to generate electricity and reduce the dependence on fossils [13, p213-215]. The United States, France	The incident damaged almost 1,000 centrifuge tubes [13, p218] in Iranian Natanz facility. This figure is significant in the light of the total number of installed tubes (9,000) and the portion of those fed with	[57], besides arguing against the media hype surrounding Stuxnet, highlights the alleged willingness of governments, both in the West and elsewhere, to deal with criminal-originated tools in cyberspace.

Games) 2009-2010[13, p212]	Israel France and Germany (on nuclear issues, not in the cyber attack) Symantec and other cybersecurity companies	Step 7 software, USB drives, Local Area Networks, and Windows vulnerabilities [13, p221]. Stuxnet spread on to over 100,000 hosts, but reportedly caused harm only to Iranian nuclear facilities [13, p218]. There, it would go on to operate the centrifuges, using drastic changes in speed to cause permanent damage. [13, p218] The virus was also designed to open and close valves, and to mask its actions by using pre-recorded normal operation indicators, thus fooling the system and the operators into thinking there was nothing unusual going on. [13, p220-221] The digital signature used by Stuxnet was renewed after Symantec discovered the virus and notified the initial issuer (Realtek) [13, p218]. DDoS attacks were launched against industrial control systems mailing lists, in order to prevent the security information related to the virus from spreading. [13, p218] Flame and Duqu are reportedly	and Germany supported this effort during the Shah's government. That support was dropped due to fears of Iran developing a nuclear weapon (the fear began before the Iranian revolution) [13, p213-215]. Clashes between Israel and Iran are not new. Former Iranian President Ahmadinejad has argued that Israel should disappear; therefore, Israel has sought support from the United States to counter Iranian nuclear weapon development [13, p216-217]. A conventional use of warfare was "politically risky", leading to the use of cyber attacks to deter Iranian nuclear program. [13, p216-217] The technical complexity and extension of the virus, along with the highly specialized information on industrial systems needed to produce it, point out to a level of sophistication only attainable by nation-state agencies [13, p223].	uranium (4,000) [13, p228]. "A 23% decline in the number of operating centrifuges from mid-2009 to mid-2010 may have been due to the Stuxnet attack." [57] Iran created a new cyber unit in its militia [13, p229]. Not much later, Comodo, a US based security firm, accused Iran of attacking several Internet giants, including Google and Microsoft [13, p229]. [57] Argues that Stuxnet used a blend of tools from the cyber crime community, and extends this to the cases in Estonia, Georgia and several others. The same paper uses that as an argument to downplay the technical sophistication of Stuxnet, its spreading mechanism, and its resilience. Furthermore, the use of third-party code increases the difficulty in the attribution of a cyber attack [57].	The high profile of this operation is shown on the willingness to attack third parties (the industrial systems mailing list [13, p218]) in order to stop defensive efforts. There are mixed reports regarding how long did Stuxnet delay Iranian procurement of a nuclear weapon. The Obama administration argued it pushed the development until at least 2015 [13, p230].

		viruses used to explore the Natanz facility in a phase previous to Stuxnet deployment [13, p219-220]. Duqu is a "Remote Access Trojan", capable of recording intelligence information on industrial facilities [13, p219-220]. Flame, which was "twenty times" bigger (file size-wise) than Stuxnet, could operate peripherals and gather several different types of information on the host and its files [13, p219-220]. Both Duqu and Flame laid the ground for Stuxnet by tampering with the target host's security settings [13, p220]. Specifically, Stuxnet targeted offline (not connected to the Internet) industrial control systems known as SCADA, an acronym for Supervisory and Control and Data Acquisitions of Siemens, by changing the code on the programmable logic controllers (PLCs) to cause the malfunction and to cover it from the operators [13, p220]. The code was changed via the Field Peripheral	Furthermore, the relatively low profile of the incident in the media, plus the specificity of the target, make anti-nuclear-weapons activists a very unlikely suspect [13, p223]. The New York Times and a "German security expert" both attribute the virus to the United States and Israel [13, p224]. They may have used their own nuclear facilities to test the virus, and information from Israeli Mossad to develop it [13, p226-227]. Edward Snowden has allegedly revealed that Stuxnet was the work of Israel and the United States [95].		

		Gateways (PG), because PLCs do not use Windows [13, p222] and thus the virus could not infect them directly. Stuxnet manipulated the centrifuges by changing the "frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed." [57] Stuxnet's code targeted very specific systems (PLCs controlling a particular type of centrifuge used in Natanz), being harmless to any other system it infected [13, p222].			
15. Wikileaks releases thousands of diplomatic cables pertaining to the US State Department and its Missions abroad 2010-2011	Wikileaks – a not for profit "transparency" organization founded and leaded by Julian Assange [11] US Department of State and other government branches and officials Dozens of other affected countries	Wikileaks publishes the cables in collaboration with selected newspapers [11]. A Senator Lieberman's (an independent) staff member allegedly threatens Amazon with an investigation, for which the company kicked WikiLeaks out (resulting in the site being temporarily down) [11]. Visa, MasterCard, Paypal and other smaller actors would follow banning WikiLeaks [11].	The US Government is arguably the most powerful government in the world. However hard they tried to stop it [11], sensitive information was still released. The above was in part due to the widespread support WikiLeaks received from open information activists or even less politically oriented people around the world [11]. This might not be the case for every	US Secretary of State – or a member of her staff – had allegedly ordered spying on UN Secretary General [11]. A Federal Court asks Twitter secretly to give in information about WikiLeaks related people [11]. Twitter asks the court to make the order public and then proceeds to inform their users of the request [11]. A similar procedure was used to seize Google email data [12]. To prevent being shut down by	Julian Assange's final goals are unclear and may even be qualified as obscure – this led members of his team to leave WikiLeaks and form OpenLeaks under a "less authoritarian" structure [11]. He, at the same time, claims he wants to change or remove "authoritarian conspiracies" (i.e. governments) [11] and is planning to run for the Australian Senate [72]. WikiLeaks is a political party there already. [72] Whichever the original

	The private sector (5 major newspapers: El Pais, Le Monde, The New York Times, The Guardian and Der Spiegel. And companies: namely Amazon, Paypal, MasterCard, Visa, Google, Twitter, Bank of America, Apple, and other smaller players) [11] Anonymous	Anonymous uses Distributed Denial of Service Attacks on the above companies' websites, bringing Visa and MasterCard's sites out for a day [11]. Senator Lieberman's website was attacked as well, as was the website of the Swedish counselor representing the women pressing sexual assault charges against Julian Assange [11].	"information openness" initiative. Twitter and Google are exceptions here – they fought back [11]. Anonymous does not have evident political clout, nor does it have clear leaders. However they have managed to scramble media and government attention by bringing down sites hostile to WikiLeaks [11]. They have allegedly been searched and some of them arrested in connection with the attacks, in the US and Europe [11].	the US Government (either by blocking via ISP, demanding the hosting company to cease doing so, or some other mean) WikiLeaks asked followers to download their data and set up *mirror sites* with over 1,000 people doing so [11]. Copies were also stored in other websites and sent (encrypted) to journalists "in case something happens to Assange or the site"[12]. Julian Assange was granted asylum by Ecuador, and is hosted by their embassy in London [83]. US and other Western governments strongly disapprove the leak, claiming "it puts lives in danger" (Assange claims he had approached them asking for which information to redact out for that purpose) [11]	intentions for the leaks are, their effect on people's trust on democratically elected governments may be significant – and they are certainly used in the rhetoric by more authoritarian regimes such as Russia and China, as [73] shows for the latter. Private companies, particularly large platforms such as Amazon, may have been more concerned about the consequences of continuing hosting WL against the government's will (this could of course do harm to their business). The major newspapers that joined in did so in the light of the information to be revealed (that's their business) but what's unusual here is their alliance with WikiLeaks. There are probably not many examples where cyber-only players have received the support of major mainstream media organizations. US spying on UN's Secretary General generated outrage, in a way presumably similar to the current reactions to NSA surveillance of US allies. This is the only case in this study

					comparable to the NSA leaks, and the US government's reaction seems to have been quite similar – i.e. discrediting the source and trying to do damage control rather than to deal openly with the issue.
16. Edward Snowden leaks information about NSA classified mass surveillance programs - 2013	The NSA and other US security agencies Edward Snowden, a former contractor of the Agency who is being sought after by the US and has been offered temporary asylum by Russia [85]. Venezuela, Bolivia and other Latin American countries	NSA captures meta-data, or accessory data to the communications (e.g. the sender/receiver), on a massive number of targets, following national security directives [88]. The Guardian (UK) and Der Spiegel (Germany) report that a number of EU and European State buildings in the US were targeted as well [86]. The NSA accessed private data stored by Yahoo, Gmail, Apple, Microsoft and other Internet giants [88]. This was done taking it directly from the Internet Service Providers [87], which made asking the platform operators (e.g. Facebook) to provide the information themselves a moot action. This made it unnecessary for the agency to even get FISA orders. Among other arguments, the leaked NSA slides claim "There were too many email accounts to be	The intention of spying on allies may be related to third countries and weapon deals, and also stopping corrupt practices such as bribery [84]. The "worry" about NSA surveillance on American citizens is not new, as shows this Congress [89] document requesting the President and the Attorney General to submit any records of NSA requesting information from phone companies without a warrant. In Germany the news of the surveillance program have been particularly unwelcome – some claim this is due to bitter memories from the Stasi [90]. Furthermore, there are elections coming up, which could lead German	European diplomats are claiming invasion to privacy and may hold back on free-trade agreement talks with US [74]. "Germany's federal prosecutor's office has also opened inquiries into the NSA debacle, with a view to establishing whether German laws have been breached."[75] There are new statements by Snowden regarding the involvement of Germany´s own government in the surveillance [76]. As [103] shows, fears of surveillance might be drawing business away from American web-related companies. A recent poll by Quinnipiac University (cited by Business Insider) suggests the American public is now more concerned on the invasion of civil liberties in the name of terrorism [26]. The incident involving Bolivian	This case marks a major difference on how the government –and, given their relatively mild reaction, also the public– see cyberspace-based information collection as opposed to more physical seizes of information. If there were to be NSA agents using telescopes to peek into people's homes (without actually getting in) the people's opposition might well be much stronger. The incident involving Bolivian president's plane can hardly be beneficial to US and European relations with the affected South American countries. It represents a reverberation of Snowden's revelations in the domain of international relations. American officials seem to be trying to brush out and downsize the implications of NSA surveillance. The NSA's argument "it would be impractical to get FISAs for

		practical to seek Fisas for all." [88]	politicians to react in a tougher way than they "normally" would. A Congressman has requested Snowden to be granted safe passage to be questioned regarding the US "espionage" programs [91]. The US has warned countries granting asylum to Snowden (most notably Venezuela) about a risk of "damaging its bilateral relations with the US." [25] Bolivian President, Evo Morales, indicated that his country "is ready to give political asylum to the people who expose spying activities" [28]. On his way back to Bolivia, his plane was denied passage over the airspace of Spain, France, Portugal and Italy, forcing the delegation to land in Vienna [28]. This led to harsh statements by several South American politicians, who suspected the move was initiated by the United States [28]. There was also condemnation by the OAS, UN, and UNASUR. [28]	President's plane, although the US was not directly – at least not officially – involved, fed some South American leaders' claims on "American Imperialism" and even neo-colonialism, as UNASUR's Cochabamba declaration shows [29]. They have demanded explanations and formal apologies from Spain, France, Portugal and Italy [29]. As this article in the Washington Post shows [32], the Bolivian plane's event's timeline is highly disputed; there is even the possibility that the plane had to land for technical reasons, and not due to any denial of access to a country's airspace [32].	all" [88] is not hard to refute; if, for example, there were to be a lead to a terrorist in a neighborhood, would it be "impractical" to get warrants before accessing dozens of houses during the lookout? What would be the people's reaction to this? And finally, why would accessing someone's house be different from accessing phone or internet content?

			US House of Representatives rejected a bill that would have limited NSA's phone surveillance capabilities [77].		
17. Hackers Intrude into New York Times 2012-2013	Hackers, allegedly Chinese, codenamed APT12 [96] China The New York Times Mandiant, a cybersecurity firm	The timespan of the attacks ranges from October 2012 to January 2013 [96], and there is evidence suggesting a new wave of attacks by the same groups on August 2013 [98]. The hackers intruded using spear-phishing, a method that involves emailing employees with malicious links, and installed remote access tools (RAT) [96]. They also routed through American universities and companies in order to disguise their identities [96]. The intruders used malware known as Aumlib and Ixeshe [101]. The second wave of attacks included updated versions of both threats [101]. In the Ixeshe case, attackers modified network traffic patterns to avoid being discovered [101]. The attackers managed to steal every employee password [96]. The New York Times hired Mandiant, after the newspaper	The New York Times is a major newspaper and website in the United States [97]. The attacks coincided with an investigation done by a New York Times journalist, exposing the alleged fortunes of Chinese prime minister Wen Jiabao's relatives [96]. In the report, the Times revealed that Wen's family "have controlled assets worth at least $2.7 billion."[100] The newspaper was threatened of "consequences" by the Chinese government [96]. The New York Times (quoting information from Mandiant, network provider AT&T, and the US Federal Bureau of Investigations) claims there is evidence linking these attacks to Chinese official institutions, including the military [96]. Given the timespan of the attacks, and the involvement	The attackers did not steal New York Times's customer data, and although they managed to penetrate the computers of 53 employees, they focused on data regarding Wen's family's wealth report [96]. Despite the significant outreach of the attacks, The Times reported "security experts found no evidence that sensitive e-mails or files from the reporting of our articles about the Wen family were accessed" [96]. The attacks stopped initially in January 2013 after the APT12 group was exposed; the exposure itself might have triggered the malware updates [101].	The New York Times is a big actor with significant political clout and a more generally widespread influence. Even as the Chinese government threatened them, they went ahead and published the controversial report on Wen's family wealth. As Mandiant (basically a contractor of The Times in this case) exposed the group, they were forced to retrieve, albeit temporarily. The above contrasts with attacks on Cybersitter (see case 9 on this paper, Chinese espionage), where the company, a much smaller player, exposed Chinese hacking but couldn't stop them from using its proprietary software. The size of the actor attacked, then, could be a factor on the success when deterring attackers from China.

		and AT&T's efforts proved insufficient [96]. The Times went to replace infected computers, "blocked the compromised outside computers, removed every back door into its network, changed every employee password and wrapped additional security around its systems." [96]	of the group in attacks to several industries, the intruders have been qualified as an advanced persistent threat (APT) by Mandiant [99].		

Appendix 3. Layers of the Internet: extract from Choucri and Clark, 2012 [104]

The Layers Architecture

We begin with a model that gives more structure and form to the Internet, which we take as the core of cyberspace. While use of a layered model to describe the Internet is well understood there is no common consensus, so we use a four-layer model that captures the features of interest for alignment purposes.

- *The physical foundations* – the Internet's bricks-and-mortar, from fiber-optic cables to cell towers, personal computers and servers.

- *The logical layer* –the Internet protocols, World Wide Web, browsers, domain-naming system, websites and software that make use of the physical foundations.

- *The information layer* –the encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace.

- *The users* – the people and constituencies who shape the cyber-experience and the nature of cyberspace itself, by communicating, working with information, making decisions and carrying out plans. Figure 2. Defining the Layers of the Internet In the layered model the upper layers depend on the functions of the lower layers, but not the opposite. This model is a useful device to (a) locate cyber actors and activities, (b) highlight significant technological changes, (c) identify the conditions under which actors operate across layers or, alternatively, chose to concentrate their activities within a layer, and (d) thus help track and represent patterns of dependencies and influence within the cyber domain.

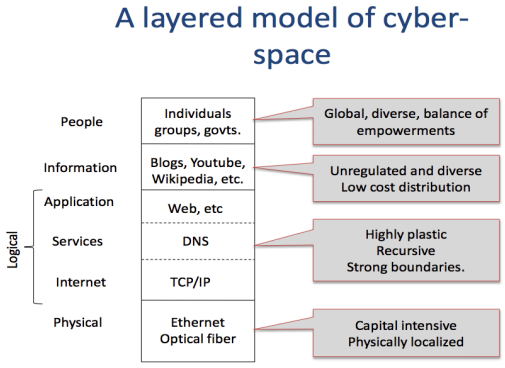

Figure 1. Defining the Layers of Cyberspace

In the layered model the upper layers depend on the functions of the lower layers, but not the opposite. This model is a useful device to (a) locate cyber actors and

activities, (b) highlight significant technological changes, (c) identify the conditions under which actors operate across layers or, alternatively, chose to concentrate their activities within a layer, and (d) thus help track and represent patterns of dependencies and influence within the cyber domain.

Appendix 4. Countries Involved in Each Case[5]

Country or International Organization	Private sector	United States	Russia	Global reach	China	Israel	NATO	The Netherlands	Germany
Case number and name									
1. Cuckoo's Egg	x	x	x						x
2. Morris Worm	x	x		x					
3. Dutch Hackers and British Hackers		x						x	
4. Operation Solar Sunrise	x	x				x			
5. Moonlight Maze	x	x	x						
6. Electronic Disturbance Theater (EDT)	x	x							
7. ILOVEYOU	x	x		x					
8. Patriotic Hackers	x	x	x		x		x	x	
9. Chinese Cyber Espionage	x	x		x	x				
10. Estonia receives cyber attacks	x		x			x	x		x
11. The Russo-Georgian War	x	x	x						
12. Agent.btz and operation Buckshot Yankee	x	x	x				x		
13. Conficker	x	x		x					
14. Stuxnet, Flame and Duqu	x	x				x			
15. Wikileaks	x	x		x					
16. Edward Snowden's NSA leaks	x	x	x	x					
17. Hackers Intrude into New York Times	x	x			x				
Frequency	**16**	**16**	**7**	**6**	**3**	**3**	**3**	**2**	**2**

Country or International Organization	Estonia	Mexico	Serbia	Iran	Phillippines	Georgia	North Korea	South Korea	Venezuela
Case number and name									
1. Cuckoo's Egg									
2. Morris Worm									
3. Dutch Hackers and British Hackers							x	x	
4. Operation Solar Sunrise									
5. Moonlight Maze									
6. Electronic Disturbance Theater (EDT)		x							
7. ILOVEYOU					x				
8. Patriotic Hackers			x						
9. Chinese Cyber Espionage									
10. Estonia receives cyber attacks	x								
11. The Russo-Georgian War						x			
12. Agent.btz and operation Buckshot Yankee									
13. Conficker									
14. Stuxnet, Flame and Duqu				x					
15. Wikileaks									
16. Edward Snowden's NSA leaks									x
17. Hackers Intrude into New York Times									
Frequency	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

[6]

Country or International Organization	Bolivia	UNASUR	United Kingdom	Finland	Slovenia	Ukraine	Hong Kong
Case number and name							
1. Cuckoo's Egg							
2. Morris Worm							
3. Dutch Hackers and British Hackers			x				
4. Operation Solar Sunrise							
5. Moonlight Maze							
6. Electronic Disturbance Theater (EDT)							
7. ILOVEYOU							
8. Patriotic Hackers							
9. Chinese Cyber Espionage							
10. Estonia receives cyber attacks				x	x		
11. The Russo-Georgian War							
12. Agent.btz and operation Buckshot Yankee							
13. Conficker						x	
14. Stuxnet, Flame and Duqu							
15. Wikileaks							
16. Edward Snowden's NSA leaks	x	x					x
17. Hackers Intrude into New York Times							
Frequency	**1**	**1**	**1**	**1**	**1**	**1**	**1**

[6] Hong Kong was the jurisdiction were Edward Snowden was before traveling to Russia.

Appendix 5. Selected Significant Cyber Incidents

This list was generated using Center for Strategic and International Studies' list on [114], using the following criteria:

- Incident is not a part of this paper.
- There is a defined target of the attack, and there is at least some suspicion about who is behind it.
- The attack transcends international borders.
- The incident refers to a specific, time-constrained and identifiable attack, and not an announcement of the type "Organization X has been attacked Y times during the last Z years."

Selected cases are shown below. A future paper will address this list using the same methodology described in this paper. In parenthesis is the bullet number of the incident in the original list [114].

1. 2006. Chinese hackers were thought to be responsible for shutting down the House of Commons computer system. (5)

2. September 2007. Israel disrupted Syrian air defense networks (with some collateral Damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility. (11)

3. January 2009. Hackers attacked Israel's Internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah. (33)

4. July 2009. Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks. The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention. (48)

5. January 2010. A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December and with a similar message. (58)

6. December 2010. British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defence contractor and other

“British interests” that evaded defenses by pretending to come from the White House. (72)

7. December 2010. India’s Central Bureau of Investigation (CBI) website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected. (73)

8. January 2011. The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada’s main economic agencies, to disconnect from the Internet. Canadian sources attribute the attack to China. (76)

9. March 2012. The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC’s Director General blamed Iran for the incident. (99)

10. March 2012. India’s Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government websites had been compromised from December 2011 to February 2012. Most of the incidents involved website defacement and many of the hacks appeared to originate in Pakistan. (100)

11. April 2012. Iran was forced to disconnect key oil facilities after a cyber attack against internal computer systems. The malware was found inside the control systems of Kharg Island – Iran’s main oil exporting terminal. Equipment at Kharg Island and at other Iranian oil plants has been disconnected from the Internet as a precaution. Iran reported that oil production was not affected, but the websites of the Iranian oil ministry and national oil company were forced offline and data about users of the sites was taken as a result of the attack. (102)

12. August 2012. A group called "Cutting Sword of Justice" linked to Iran claimed it has used the “Shamoon” virus to attack Aramco, a major Saudi oil supplier, deleting data on 30,000 computers and infecting (without causing damage) control systems. The attack also affected the Qatar company RasGas, a major LNG supplier. Other oil companies may have also been infected. (115) AND January 2013.

13. September 2012. Izz ad-Din al-Qassam, a hacker group linked to Iran,

launched “Operation Ababil” targeting bank websites for sustained denial-of-service attacks. Targets include Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, and Regions Bank. (116) Izz ad-Din al-Qassam claims responsibility for another series of distributed denial-of-service attacks against US Bank websites, as part of “Operation Ababil,” phase two. Targets include: Ally Financial, BB&T, Capital One, Fifth Third Bank, HSBC, PNC, Wells Fargo, SunTrust, and Zions Bank. US officials speculate that the group is a front for a state-sponsored campaign attributed to Iran. (121)

14. December 2012. Al-Qaida websites were taken off line for two weeks. This follows a 2008 website disruption aimed at damaging recruiting and propaganda efforts by the group. (119)

15. March 2013. North Korea blames the United States and South Korea for a series of attacks that severely restricted Internet access in the country. (128)

16. March-June 2013. The Syrian Electronic Army, a pro-Assad hacktivist group, hacked into major Western media organizations as part of a propaganda campaign. (131)

17. May 2013. And unknown attacker utilized a DDoS attack to bring down the website of the Iranian Basij military branch (basij.ir). (135)

18. May 2013. Anonymous’ Saudi branch launches OpSaudi and takes down several government web sites such as the Ministry of Foreign Affairs, Ministry of Finance, and the General Intelligence Presidency via DDos attack. (137)

19. May 2013. Israeli officials report a failed attempt by the Syrian Electronic Army to compromise water supply to the city of Haifa. (143)

20. June 2013. On the 60th Anniversary of the Korean War, a wave of cyber-incidents in Korea began involving South Korea, North Korea, and the United States. The incidents began with DDoS attacks on major South Korean websites. North Korean websites also went down including those of the communist party and the national airlines. The US was drawn into the ongoing cyber dispute by the hacking of tens of thousands of soldiers’ personal information. (148)

References

[1] Willis H. Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1." *Office of the Secretary of Defense*, 1979. Accessed on August 2013. <http://www.rand.org/pubs/reports/R609-1/index2.html>

[2] Stoll, Clifford. "Stalking the Wily Hacker." *Commun. ACM* 31.5 (1988): 484–497. *ACM Digital Library*. Web. 30 Oct. 2013.

[3] Piore, Adam. "Digital Spies: The Alarming Race of Economic Espionage." *Popular Mechanics*. Accessed on August 2013. <http://www.popularmechanics.com/technology/how-to/computer-security/digital-spies-the-alarming-rise-of-electronic-espionage>

[4] Kehoe, Brendan P. "The Robert Morris Internet Worm." *Computer Science and Artificial Intelligence Laboratory*. N.p., n.d. Web. 03 Nov. 2013. <http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html>

[5] "The Cornell Commission: On Morris and the Worm." 1989 *Communications of the ACM*. Jun89, Vol. 32 Issue 6, p706-710. 5p.

[6] "Hacking U.S. Government Computers from Overseas." *United States Department of Agriculture*. Accessed on August 2013. <http://www.dm.usda.gov/ocpm/Security%20Guide/Spystory/Hacking.htm>

[7] "609 IWS: A Brief History Oct 1995-Jun 1999." *SecurityCritics.org*. Accessed on August 2013. <http://securitycritics.org/wp-content/uploads/2006/03/hist-609.pdf>

[8] "Hacktivism: Means and Motivations … What Else?" *InfoSec Institute*. N. p., n.d. Web. 4 Nov. 2013. <http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/>

[9] "Cyber Attack! July 3 2000." *BBC* 3 July 2000. *bbc.co.uk*. Web. 4 Nov. 2013. <http://news.bbc.co.uk/2/hi/programmes/panorama/817114.stm>

[10] "From the WSJ Opinion Archives." *The Wall Street Journal*. 14 Nov. 2007. Web. 4 Nov. 2013. <http://online.wsj.com/news/articles/SB123749361171887785>

[11] Sifry, Micah L. "WikiLeaks and the Age of Transparency." 2011.

[12] "WikiLeaks Backup Plan Could Drop Diplomatic Bomb." *CBS News*. 3 Dec. 2010. Web. 4 Nov. 2013.

[13] Healey, J. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. *Atlantic Council*. Cyber Conflict Studies Association. 2013.

[14] "A Filipino Linked To Love Bug Talks About His License To Hack." *The New York Times*, 2000. Accessed on August 2013. <http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html?ref=oneldeguzman>

[15] "Love Bug revenge theory." *BBC News*, 2000. Accessed on August 2013. <http://news.bbc.co.uk/2/hi/science/nature/743082.stm>

[16] George V. Hulme. "A Decade Ago, ILoveYou Worm Changed Security." *Information Week*, 2010. Accessed on August 2013. <http://www.informationweek.com/security/a-decade-ago-iloveyou-worm-changed-secur/229202714>

[17] Buckland, Jason. "10 Worst Cybercrimes of the Decade." *msn Canada*, n.d. Web. 03 Nov. 2013. <http://tech.ca.msn.com/photogallery.aspx?cp-documentid=27611570>.
[18] Sprinkel, Shannon C. "Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime." *Suffolk Transnational Law Review*, Vol. 25, Issue 3 (Summer 2002), pp. 491-514
[19] "Computer Bug Infects UK Parliament." *Express India*, 2000. Accessed on August 2013. <http://expressindia.indianexpress.com/news/ie/daily/20000505/iin05063.html>
[20] "A Brief History of Malware; The First 25 Years." *About.com*. Accessed on August 2013. <http://antivirus.about.com/od/whatisavirus/a/A-Brief-History-Of-Malware-The-First-25-Years_2.htm>
[21] "Press Release: Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison" (May 1, 2002). *U.S. Department of Justice*. Accessed on August 2013. <http://www.justice.gov/criminal/cybercrime/press-releases/2002/melissaSent.htm>
[22] "U.S. catches 'Love' virus." *CNN Money*, May 5, 2000. Accessed on August 2013. <http://money.cnn.com/2000/05/05/technology/loveyou/>
[23] "Exterminator: Microsoft to patch Outlook in wake of ILOVEYOU worm." *Tech Republic*, June 8, 2007. Accessed on August 2013. <http://www.techrepublic.com/article/exterminator-microsoft-to-patch-outlook-in-wake-of-iloveyou-worm/1033403>
[24] "ECIR Project Review, 2013." *Massachusetts Institute of Technology* and *Harvard University*.
[25] "US Warns Venezuela Against Accepting Snowden." *RTT News*, July 9, 2013. Accessed on August 2013. <http://www.rttnews.com/2147582/us-warns-venezuela-against-accepting-snowden.aspx>
[26] "Edward Snowden's Leaks Have Caused A 'Massive Shift' In The Public's Views Of Government Surveillance." *Business Insider*, July 10, 2013. Accessed on August 2013. <http://www.businessinsider.com/edward-snowden-poll-nsa-surveillance-asylum-venezuela-2013-7>
[27] "Serbs launch cyberattack on NATO." *FCW*, April 4, 1999. Accessed on August 2013. <http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx>
[28] "Evo Morales' plane grounding causes uproar throughout Latin America." *Fox News Latino*, July 10, 2013. Accessed on August 2013. <http://latino.foxnews.com/latino/politics/2013/07/10/bolivia-plane-grounding-causes-uproar-throughout-latin-america/>
[29] "Declaracion de Cochabamba: La UNASUR exige disculpas a España, Portugal, Italia y Francia." *Argentinian President's Office* (Spanish), July 4, 2013. Accessed on August 2013. <http://www.prensa.argentina.ar/2013/07/05/42197-declaracion-de-cochabamba--la-unasur-exige-disculpas-publicas-a-espana-portugal-italia-y-francia.php>

[30] "Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says." *CNN*, May 12, 1999. Accessed on August 2013. <http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg/>
[31] "Cyber Protests: The Threat to the U.S. Information Infrastructure." *National Infrastructure Protection Center*, October 2001. Accessed on August 2013. <http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.htm>
[32] "Evo Morales' Controversial Flight Minute by Heavily Disputed Minute." *The Washington Post*, July 7, 2013. <http://www.washingtonpost.com/blogs/worldviews/wp/2013/07/03/evo-morales-controversial-flight-over-europe-minute-by-heavily-disputed-minute/>
[33] "Cybersitter Sues China for Piracy." *Financial Times*, January 6, 2010. Accessed on August 2013. <http://www.ft.com/cms/s/2/3ad29902-fa81-11de-a532-00144feab49a.html#axzz2YrLFbtBo>
[34] "Cybersitter's Battle Against Chinese Hackers." *Socaltech.com*. Accessed on August 2013. <http://www.socaltech.com/cybersitter_s_battle_against_chinese_hackers/s-0046458.html>
[35] Matusitz, Jonathan. "Social Network Theory: A Comparative Analysis of the Jewish Revolt in Antiquity and the Cyber Terrorism Incident over Kosovo." *Information Security Journal: A Global Perspective*, 20:34–44, 2011.
[36] "Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)." *YouTube.com* (video). Accessed on August 2013. <https://www.youtube.com/watch?v=VVJldn_MmMY>
[37] "China's Growing Middle Class." *CNN Money*, April 26, 2012. Accessed on August 2013. <http://money.cnn.com/2012/04/25/news/economy/china-middle-class/index.htm>
[38] "The World Factbook." *Central Intelligence Agency*. N.p., n.d. Web. 03 Nov. 2013. <https://www.cia.gov/library/publications/the-world-factbook/fields/2195.html>.
[39] "China is Seeking U.S. Assets." *The Wall Street Journal*, May 20, 2013. Accessed on August 2013. <http://online.wsj.com/article/SB10001424127887324787004578494632401290050.html>
[40] "The CIO's Nightmare: Intellectual Property Lawsuits." *HP Print Input Output*, December 28, 2011. Accessed on August 2013. <http://h30565.www3.hp.com/t5/Feature-Articles/The-CIO-s-Nightmare-Intellectual-Property-Lawsuits/ba-p/1168>
[41] "Why China Might Never Protect IP." *Harvard Business Review* (Blog), 2013. August 2013. <http://blogs.hbr.org/hbr/meyer-kirby/2010/07/why-china-might-never-get-arou.html>
[42] Peter L. Mattis (2012). "Assessing Western Perspectives on Chinese Intelligence," *International Journal of Intelligence and CounterIntelligence*, 25:4, 678-699, DOI: 10.1080/08850607.2012.678745
[43] "Overview." *United States House of Representatives*, n.d. Web. 03 Nov. 2013. <http://www.house.gov/coxreport/chapfs/over.html>.
[44] "Distributed Denial-of-service Attack (DDoS)." *SearchSecurity*.

TechTarget, May 2013. Web. 04 Nov. 2013. <http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>.
[45] "SYN Flood." *Internet Security Systems*. IBM, n.d. Web. 04 Nov. 2013. <http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm>
[46] Herzog, Stephen. 2011. *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. Journal of Strategic Security, 4 (2): 49-60.
[47] Clarke, Richard and Knake, Robert. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins Publishers.
[48] "The "Bronze Night" Cost Estonia over 4mn Euro." *Regnum - Russian News*. Regnum News Agency, 27 July 2007. Web. 04 Nov. 2013. <http://www.regnum.ru/english/862457.html>.
[49] "What Is SQL Injection and How to Fix It." *Acunetix*. N. p., n.d. Web. 4 Nov. 2013. <http://www.acunetix.com/websitesecurity/sql-injection/>
[50] Clarke, Justin. "Chapter 1 - What Is SQL Injection?". *SQL Injection Attacks and Defense*. Syngress Publishing. © 2009.
[51] Gupta, S. and Sharma, L. "Exploitation of Cross-Site Scripting (XSS) Vulnerability on Real World Web Applications and its Defense." *International Journal of Computer Applications* 60(14):28-33, December 2012. Published by Foundation of Computer Science, New York, USA.
[52] "The 10 Most Powerful Militaries In The World." *Business Insider*, June 12, 2013. Accessed on August 2013. http://www.businessinsider.com/10-most-powerful-militaries-in-the-world-2013-6?op=1
[53] Swanson, Lesley. 2010. "The Era Of Cyber Warfare: Applying International Humanitarian Law To The 2008 Russian-Georgian Cyber Conflict." *Loyola Of Los Angeles International & Comparative Law Review* 32, 303.
[54] Canan, James W. "Defending Against Cyber Threats." *Aerospace America.* Oct 2011, Vol. 49 Issue 9, p22-41. 7p.
[55] "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012." *Atlantic Council.* Accessed on July 2013. www.acus.org/afiercedomain
[56] "Estonia's Return to Independence 1987–1991." *Estonia.eu*. N.p., n.d. Web. 04 Nov. 2013. <http://estonia.eu/about-estonia/history/estonias-return-to-independence-19871991.html>.
[57] Farwell, J. P., & Rohozinski, R. (2011). "Stuxnet and the Future of Cyber War." *Survival (00396338)*, *53*(1), 23-40.
[58] Porras, Phillip. 2009. "Inside Risks: Reflections on Conficker." *Communications Of The ACM* 52, no. 10: 23-24.
[59] Markoff, John. "Worm Infects Millions of Computers Worldwide." *The New York Times* 23 Jan. 2009. *NYTimes.com*. Web. 4 Nov. 2013.
[60] "Lotte Senza Confini. L'electronic Disturbance Theatre 2.0" (Italian). *Digimag*, 2011. Accessed on July 2013. http://www.digicult.it/it/digimag/issue-062/no-borders-struggles-the-electronic-disturbance-theatre-2-0/
[61] "FloodNet Foyer." *Thing.net*. Accessed on July 2013. http://www.thing.net/~rdom/zapsTactical/foyer3.htm

[62] "'Virtual sit-in' tests line between DDoS and free speech." *The Register* (UK), 2010. Accessed on July 2013. http://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/
[63] "Electronic Civil Disobedience." *Thing.net*, 2008. Accessed on July 2013. http://www.thing.net/~rdom/ecd/ecd.html
[64] Kremen, Stanley. "Apprehending The Computer Hacker: The Collection and Use of Evidence." *Computer Forensics Online*, 1998. Accessed on July 2013. http://www.shk-dplc.com/cfo/articles/hack.htm
[65] "Hacker Case Taps Into Fame, Fury." *Los Angeles Times*, 1998. Accessed on July 2013. http://articles.latimes.com/1998/apr/27/news/mn-43491
[66] "'The Analyzer' Hack Probe Widens; $10 Million Allegedly Stolen From U.S. Banks." *Wired.com*, 2009. Accessed on July 2013. http://www.wired.com/threatlevel/2009/03/the-analyzer-ha/
[67] "Solar Sunrise." *Globalsecurity.org*, 2011. Accessed on August 2013. http://www.globalsecurity.org/military/ops/solar-sunrise.htm
[68] "Newsweek Exclusive: 'We're in the Middle of a Cyberwar.'" *PR Newswire*. Accessed on August 2013. http://www.prnewswire.com/news-releases/newsweek-exclusive-were-in-the-middle-of-a-cyberwar-74343007.html
[69] See *supra* at 55.
[70] "Interview John Arquilla." *PBS Frontline*, 2003. Accessed on July 2013. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html
[71] Carroll, Amy. 2003. "Incumbent Upon Recombinant Hope. EDT's Strike a Site, Strike a Pose" *The Drama Review*, MIT Press.
[72] "Wikidemocracy: Julian Assange's Wikileaks Party Could Win Senate Seat In Australia." *Occupy.com*, 2013. Accessed on August 2013. http://www.occupy.com/article/wikidemocracy-julian-assange's-wikileaks-party-could-win-senate-seat-australia
[73] "China's Reaction To The NSA Leaks Has Been All Over The Map." *Business Insider*, 2013. Accessed on August 2013. http://www.businessinsider.com/chinese-awareness-of-nsa-leaks-and-snowden-2013-6
[74] "Barack Obama seeks to limit EU fallout over US spying claims." *The Guardian* (UK), 2013. Accessed on August 2013. http://www.guardian.co.uk/world/2013/jul/01/barack-obama-eu-fallout-us-spying-claims
[75] "NSA spying row: bugging friends is unacceptable, warn Germans." *The Guardian* (UK), 2013. Accessed on August 2013. http://www.guardian.co.uk/world/2013/jul/01/nsa-spying-allegations-germany-us-france
[76] "Snowden Interview: NSA and the Germans 'In Bed Together.'" *Spiegel Online*, 2013. Accessed on August 2013. http://www.spiegel.de/international/world/edward-snowden-accuses-germany-of-aiding-nsa-in-spying-efforts-a-909847.html

[77] "US House votes to continue NSA's phone surveillance." *BBC*, 2013. Accessed on August 2013. http://www.bbc.co.uk/news/world-us-canada-23445231
[78] O'Malley, C. "Information warriors of the 609th." *Popular Science*, (1997, 07), 251, 70-74
[79] See *supra* at 67.
[80] See *supra* at 70.
[81] Tompkins, Michael. "Computer Network Defense at the National Level." Indiana University of Pennsylvania, 2000. Accessed on August 2013. http://www.lib.iup.edu/comscisec/SANSpapers/tompkins.htm
[82] "Joint Task Force On Computer Network Defense Now Operational." *U.S. Department of Defense*, 1998. Accessed on August 2013. http://www.defense.gov/releases/release.aspx?releaseid=1945
[83] "Julian Assange stakeout at Ecuadorean embassy costs Met police £3.8m." *The Guardian* (UK), 2013. Accessed on August 2013. http://www.guardian.co.uk/media/2013/jul/10/julian-assange-ecuadorian-embassy-police-cost
[84] "Intel insiders: Europeans spying on us, too." *CBS News*, 2013. Accessed on August 2013. http://www.cbsnews.com/8301-202_162-57591922/intel-insiders-europeans-spying-on-us-too/?pageNum=2
[85] "Edward Snowden asylum: US 'disappointed' by Russian decision." *The Guardian* (UK), 2013. Accessed on August 2013. http://www.theguardian.com/world/2013/aug/01/edward-snowden-asylum-us-disappointed
[86] "The lives of others." *The Economist*, 2013. Web. Accessed on August 2013. http://www.economist.com/news/leaders/21580464-european-governments-should-not-kick-up-fuss-about-american-spying-they-have-too-much?fsrc=scn/fb/wl/pe/thelivesofothers
[87] "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian* (UK), 2013. Web. Accessed on August 2013. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data
[88] "NSA slides explain the PRISM data-collection program." *The Washington Post*, 2013. Web. Accessed on August 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
[89] "President and directing the Attorney General to submit to the House of Representatives all documents in the possession of the President and the Attorney General relating to requests made by the National Security Agency and other federal agencies to telephone service providers requesting access to telephone communications records of persons in the United States and communications originating and terminating within the United States without a warrant." [electronic resource] report (to accompany H. Res. 819). (2006). [Washington, D.C. : U.S. G.P.O., 2006].
[90] "Germans Hail Snowden as NSA Evokes Stasi Seizing Lives of Others." *Bloomberg*, 2013. Accessed on August 2013.

http://www.bloomberg.com/news/2013-07-10/germans-hail-snowden-as-nsa-evokes-stasi-seizing-lives-of-others.html
[91] "Politician: Call Snowden to Germany as witness." *Thelocal.de* (English version), 2013. Accessed on August 2013.
http://www.thelocal.de/national/20130704-50697.html
[92] "UNITED STATES of America, Appellee, v. Robert Tappan MORRIS, Defendant-Appellant." *United States Court of Appeals*, 1991. Accessed on August 2013. http://www.loundy.com/CASES/US_v_Morris2.html
[93] Markoff, John. "Vast Spy System Loots Computers in 103 Countries." *The New York Times* 29 Mar. 2009. *NYTimes.com*. Web. 4 Nov. 2013.
[94] "Google Aurora Hack Was Chinese Counterespionage Operation." *Information Week*, 2013. Accessed on August 2013. http://www.informationweek.com/security/attacks/google-aurora-hack-was-chinese-counteres/240155268
[95] "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet." *ABC News*, 2013. Accessed on August 2013.
http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/
[96] "Hackers in China Attacked The Times for Last 4 Months." *The New York Times*, 2013. Accessed on August 2013.
http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0
[97] Adams, Russell. "New York Times Readies Pay Wall." *The Wall Street Journal*. 24 Jan. 2013. Web. 4 Nov. 2013.
[98] "Hackers Who Attacked New York Times Are At It Again, FireEye Says." *DarkReading.com*, 2013. Accessed on August 2013.
http://www.darkreading.com/attacks-breaches/hackers-who-attacked-new-york-times-are/240159867
[99] "Chinese Military Tied To Major Cyberespionage Operation." *DarkReading.com*, 2013. Accessed on August 2013.
http://www.darkreading.com/attacks-breaches/chinese-military-tied-to-major-cyberespi/240148807?pgno=1
[100] "Billions in Hidden Riches for Family of Chinese Leader." *The New York Times*, 2012. Accessed on August 2013. http://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html?_r=0&adxnnl=1&pagewanted=all&adxnnlx=1376521119-dFVDBmzNYJvCqA4JhW0w0A
[101] "Survival of the Fittest: New York Times Attackers Evolve Quickly." *FireEye.com*, 2013. Accessed on August 2013. http://www.fireeye.com/blog/technical/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html
[102] "Update: Ukraine Disrupts $72M Conficker Hacking Ring." *Computer World*, 2011. Accessed on August 2013.
http://www.computerworld.com/s/article/9217872/Update_Ukraine_disrupts_72M_Conficker_hacking_ring

[103] "NSA Could Drive $35 Billion Away from US Cloud Providers by 2016." *The Web Host Industry Review*, 2013. Accessed on August 2013. < http://www.thewhir.com/web-hosting-news/nsa-could-drive-35-billion-away-from-us-cloud-providers-by-2016>.
[104] Choucri, Nazli and Clark, David. "Integrating Cyberspace And International Relations, The Co-Evolution Dilemma." *MIT Political Science Department* Research Paper No. 2012-29, SSRN. November 2012.
[105] Poulsen, Kevin, and 15th June 2001. "Solar Sunrise Hacker 'Analyzer' Escapes Jail." *The Register*. 15 June 2001. Web. 4 Nov. 2013. <http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/>
[106] See *supra* at 71.
[107] McKay, Niall. "Pentagon Deflects Web Assault." *WIRED*. 9 Oct. 1998. Web. 4 Nov. 2013. <http://www.wired.com/politics/law/news/1998/09/14931>
[108] "Meet the WikiLeaks Guy Who Got His Gmail Seized by the Feds." *Mother Jones*. 25 June. 2013. Web. 4 Nov. 2013. <http://www.motherjones.com/politics/2013/06/herbert-snorrason-wikileaks-google-assange>
[109] Arnold, Wayne. "TECHNOLOGY; Philippines to Drop Charges on E-Mail Virus." *New York Times*. 22 Aug. 2000. Web. 4 Nov. 2013.
[110] "Filter ICMP Packets." *Camber.com*. Camber, n.d. Web. 4 Nov. 2013. <http://www.camber.com/pdf/cybersecurity/sc/Filter_ICMP_packets.pdf>.
[111] "Öine Märul: Üks Surnu, 57 Vigastatut, 99 Lõhkumisjuhtu Ja 300 Kinnipeetut - Eesti Uudised - Postimees.ee." *Postimees* (Estonian). 27 Apr. 2007. Web. 4 Nov. 2013.
[112] "Conficker." *ShadowServer*. Shadowserver Foundation, n.d. Web. 4 Nov. 2013. <http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker>.
[113] "Help Protect Yourself from the Conficker Worm." *Microsoft.com*. Microsoft, n.d. Web. 04 Nov. 2013. <http://www.microsoft.com/security/pc-security/conficker.aspx>.
[114] Lewis, J. (2013). *Significant Cyber Incidents Since 2006*. Center for Strategic and International Studies.
[115] *TargetMap*. N. p., 2013. <http://www.targetmap.com/>