LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

FACOLTA' DI ECONOMIA E FINANZA
CORSO DI LAUREA IN ECONOMICS AND BUSINESS
CATTEDRA DI LAW AND ECONOMICS

The Economics of Cyberterrorism: The Many Sides of the Prism

Relatore
Professor Andrea Renda

Candidato
Cecilia Pupillo
Matricola: 161841

Anno Accademico 2012/2013

Table of Contents

1. Introduction 4

1.1 From the cold war to the code war 4

1.2 The geopolitics of cyber war 6

1.3 Cybercrime, Cyber Warfare and Cyberterrorism: origins and definitions 7

1.4 Focus on cyberterrorism 9

Box 1.1 Cyberterrorist attacks..... 12

2. The impact of Cyberterrorism 11

2.1 How do cyber warriors and cyberterrorists strike? 13

Box 2.1 Increasing sophistication of cyber security threats: the case of Stuxnet..... 17

Box 2.2 Advanced Persistent Threats 1 (APT1) 18

2.2 What is the scale of these strikes? 19

2.3 What is the economic impact of these strikes? 27

2.3.1 *Estimated loss from cybercrime* 28

2.3.2 *Effect of cyber attacks on stock prices* 28

2.3.3 *Insurance industry and cyber-attack risks* 31

2.3.4 *Macroeconomic effects of cyber-attacks* 31

2.4 What is the economic impact of cyberterrorism? 32

3. The response to Cybercrime and Cyberterrorism 35

3.1 Cybersecurity as risk management 35

3.2 An efficient level of cybersecurity 39

3.3 Fight against cyberterrorism and international cooperation 42

3.4 Insuring against cyber risks 43

3.5 The role of National Cyber Security Strategies (NCSS) 43

3.6 National Cybersecurity Strategies in Europe 44

3.7 European Union Cybersecurity Strategy 46

3.7.1 *Achieving cyber resilience* 46

3.7.2 *Drastically reducing cybercrime.* 47

3.7.3 *Developing cyberdefence policy and capability related to the framework of the Common Security and Defence Policy (CSDP)* 48

3.7.4 *Developing industrial and technological resources for cybersecurity* 48

3.7.5 *Establishing a coherent international cyberspace policy for the European Union and promoting EU core values* 49

3.8 Cyber Security Strategies of non EU countries 49

3.8.1 *United States of America* 49
3.8.2 *Canada* 50
3.8.3 *Japan* 50
3.9 Cyber space global governance and response to cybercrime and cyberterrorism 50

4. Conclusions 53

5. Bibliography 59

1. Introduction

1.1 From the cold war to the code war

"It is fair to say that we're already living in an age of state-led cyber war, even if most of us aren't aware of it […]. The logical conclusion of many more states coming online, building or buying cyber-attack capability and operating within competitive spheres of online influence is perpetual, permanent, low-grade cyber war."[1]

The words of Eric Schmidt, CEO of Google, and Jared Cohen, Director of Google Ideas, set the stage for understanding how the cyberspace is becoming the realm of a political battle worldwide.

Why is it happening? The Internet today is at the center of economic activity and social life of enterprises and citizens. Every day, it becomes more important and more pervasive thanks to the massive investment in infrastructure made by the telcos, hundreds of thousands of applications and services made available by the internet ecosystem of companies and developers, the development of high speed mobile internet access, cloud computing and ubiquitous computing. We no longer need to go on the Internet because we live in the Internet.

The Internet and communications infrastructure are becoming a key platform to conduct business, connect people and provide government services. But, it is its very global nature that is making the Internet everyday more important: any Internet services block or denial have major economic impacts.

The Internet is considered today a critical infrastructure because it serves communications between communities, businesses, industrial and distribution entities, medical and emergency services, military operation as well as air and sea traffic control systems. It is so important to our western way of life that it is a viable target for those seeking to assert their influence and agendas on the rest of humanity.[2] The reliance on the Internet creates opportunities for cyber-attacks.

In the last years, there has been an escalating sequence of cyber-attacks involving, in some cases, millions of people across the Internet. According to Geoff Dyer, director of the US National Intelligence, "cyber-attacks are now the most pressing threat to the US security, ahead of Islamist terrorism."[3] Although estimating the annual worldwide loss to cybercrime has been a challenge, the

[1] Schmidt and Cohen, *New Digital Age*, 104.
[2] See Curran et al. in Janczewski and Colarik, eds., *Cyber Warfare*, 1-6.
[3] "Intelligence Chief in US Cyber-attack Warning," *Financial Times*, March 13, 2013.

most often cited figure for this phenomenon is US$1 trillion.[4] Furthermore, according to the 2011 *Norton Cybercrime Report*, 69% of the world's Internet users have been victimized by cyber-criminals' activity at some point in their life.

The rate of growth and sophistication in cyber-attacks has affected national interests and required governments to adjust their national security and national defense strategies. According to a 2007 Report by the FBI, 108 countries had established offensive cyber warfare capabilities. Among the countries with the most offensive cyber warfare capabilities, other surveys mention the USA, China, Russia and Israel.[5]

Often, cybercrime is associated with an increasing weigh of financial losses, intellectual property theft, breach of privacy as well as other social outcomes. Consequently, cybercrime and cybersecurity are playing an increasing strategic role in international relations and politics. The globalization of crime has created new players and redefined the power in international relations and politics. As described by Markoff, the conflict between the states and non-states criminal groups is "the new war of globalization." [6] Therefore, global governance mechanisms of cyberspace are assuming an increasingly important role in shaping cyber security issues and fighting cybercrime.

In this regard, the murky conclusions of the Dubai WCIT (World Conference on International Telecommunications) in 2012 are seen by some observers as the beginning of a new digital Cold War that will increase the threat of cyber wars across Internet. The United States delegation, after days of negotiation, left the Conference without signing the final Treaty on the assumption that the Treaty may jeopardize the freedom of the Internet.[7]

Actually, the result of the WCIT is only the latest step of a struggle between different views of the global governance of the cyberspace. Currently, there is a conflict between countries supporting a greater role of the ITU and those supporting the current model of Internet governance centered on that the US based Internet Corporation for Assigned Names and Numbers (ICANN) - a private not for profit organization incorporated in the USA. While the governments of the United States and the EU are convinced that ICANN should continue to be the main organization in the Internet governance process, some countries like Russia, China, Brazil, South Africa, India and some Middle East Economies and Arab States would like the ITU to offer not only technical support in the Internet governance process but become a forum for discussion of the Internet

[4] See Ksetri, *Cybercrime and Cybersecurity*, 1.
[5] See Markoff, "A Code for Chaos".
[6] See Ibid., 4.
[7] See ITU, *ITR Final*.

governance issues, since they perceive ICANN as a means to put the United States in a privileged position to regulate and oversee the Internet.

According to some observers, at the WCIT, the hard line position of the US and some Western allies was led by some sort of ITU-phobia. To some, the ITU represents a special, persistent and enormously powerful threat to the Internet and its freedom. "ITU phobia is a feverish, diseased way of thinking about the ITU role in Internet governance. It seems to be communicable, with outbreaks in Dubai spreading from the US delegation to Canada, the UK and parts of Europe."[8]

Yet, differences do exist in the motivations among the countries supporting the ITU. While some countries such as China or Russia want to control the Internet, even through forms of censorship, there are other nations that side with the ITU because they feel having no voice in the ICANN governed Internet.

To sum up the debate, such a reciprocal lack of trust is often one of the biggest roadblocks for fighting cybercrime and has contributed to generate strong geopolitical rivalry.[9]

1.2 The geopolitics of cyber war

Cyber war has been brewing in the last two three years and although it might be viewed as governments going head to head in a shadow fight, security experts believe that the battleground is shifting from government entities to the private sector and to civilian targets that provide many essential services to citizens.[10]

The cyber war has seen various attacks around the world, with incidents such as Stuxnet, Flame and Red October capturing people's attention. U.S. entities are being targeted by social-agenda 'hacktivist' groups, such as Anonymous, and very skilled criminal hackers on multiple fronts: in China and Iran for espionage and intellectual property theft; in Russia and Eastern Europe for syndicated crime such as stealing cash and identities.

A new instance of such a war is going on between United States and Israel on one side and Iran on the other. According to the *New York Times*, for example, Stuxnet was developed by Israel, with U.S. support, to hobble Iranian facilities. It appeared in the second half of 20l0 and was designed to attack Siemens industrial control computers that were used in oil pipelines, nuclear plants and power grids. However, the worm damaged also the operations of industrial control

[8] See Mueller, "ITU Phobia".
[9] See Kshetri, *Cybercrime and Cybersecurity*, 203.
[10] See Violino, "Unseen, All-out Cyber War".

computers in plants in China, India and Indonesia.[11] Considering the Stuxnet worms' unusual sophistication and complexity, *The Economist* suggested that it was created by well-funded and particularly knowledgeable computer experts.[12] Furthermore, according to Microsoft, the creation of the virus took 10.000 man-days of works by top rank software engineers.[13] This worm was created under the program Olympic Games started by the Bush Administration and was continued by the Obama Administration even after a programming error made public part of the program in 20l0.

Iran has hit back with cyber-attacks on U.S. banks. Furthermore, Iran may have also been behind the Shamoon virus that attacked 30,000 hard drives and put down computers for weeks at the oil producer Saudi Aramco. In 2011, Iran was also the source of an attack on the Dutch certificate authority DigiNotar. It compromised the certificate system that enables Internet users to check and trust the identity of websites they visit and the source of communications they receive.

In the past six months of the current year, we have seen cyber-attacks to oil and gas companies in the Middle East, on US Banks including Bank of America, HSBC, and Citigroup. On March 2013 North Korea suffered an Internet outage and blamed the U.S, while South Korean Banks and the natural gas company claimed to be victim of cyber-attacks as well.[14]

Also Chinese cyber-attacks have become so intense lately that they threaten the relationship between Washington and Beijing. According to *The Economist*, China's state-sponsored hackers are ubiquitous and totally unabashed.[15] Therefore, cyber war concerns played a big role in the recent informal US-China talks between Obama and the Chinese president Xi Jinping, in California.

1.3 Cybercrime, Cyber Warfare and Cyberterrorism: origins and definitions

Before analyzing the economic dimension of these phenomena, it is worthwhile to discuss in more detail the meaning of the phenomena starting from a formal definition. According to Colarik and Janzewski (2008), the term cyberterrorism was coined in 1996 by combining the terms cyberspace and terrorism.[16] This term has been widely adopted after being embraced by the United States Armed Forces: *cyberterrorism means premeditated, politically motivated attacks by sub*

[11] Markoff, "A Code for Chaos".
[12] See *The Economist* 20l0.
[13] See Dickey et al., *Newsweek* 2010.
[14] *CircleID* 2013.
[15] See *The Economist* 2013.
[16] Most of this section draws on Janzewski and Colarik, eds., *Cyber Warfare*.

national groups or clandestine agents or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets.

While cyber warfare *is defined as a planned attacks to nations or their agents against information and computer systems, computer programs, and data that results in enemy loss.*

Why do cyber warriors and cyberterrorists strike? The most probable reasons for cyber-attacks are:

- **Fear factor:** the most common denominator of the majority of terrorist attacks is a terrorist wishes the creation of the fear in individuals, groups, or societies. The same applies to attacks against IT installations and more in general to critical infrastructures.
- **Spectacular factor:** whatever is the actual damage of an attack, it should have a spectacular nature. By spectacular we consider attacks aimed at either creating huge direct losses and/or resulting in a lot of negative publicity.
- **Vulnerability factor:** cyber activities do not always end up with huge financial losses. Some of the most effective ways to demonstrate an organization's vulnerability is to cause a denial of service to the commercial server or something as simple as the defacement of an organization's web pages, very often referred to as computer graffiti.

In practice, the difference between cyber warfare and cyberterrorism is that cyberterrorism causes fear and damage to anyone in the vicinity, while cyber warfare has a defined target in a war (ideological or declared). Furthermore, quite often the term *cybercrime* is used by the law enforcement agencies to mean a crime committed through the use of information technology.

It is important to point out that the physical forms of cyberterrorism, cyber warfare and cybercrime often look very much alike. The real difference lays **in the intention of the attacker.** Colarik and Janzewski give a good example to make this argument clear.

Suppose that an individual gains access to the online hospital's medical database with the intention of altering the medical records and possibly causing the death of a patient who happens to be an executive of a weapons company. If the act causes death, which definition applies? It depends on the intention that drove the action of the individual. If it was intentionally done, it would be murder in addition to cybercrime. If the executor would admit of doing it again, were his/her demands would have not be met, then it could be considered cyberterrorism. If finally, the actions were conducted by an agent of a foreign power, then it could be labeled cyber warfare.

The distinction between the terms is extremely important in order to design a comprehensive strategy against cyberterrorism and cyber warfare that takes into account also non-technological issues and analyzes contextual elements useful to understand the causes of this phenomenon.

1.4 Focus on cyberterrorism

Given the complex nature of the phenomenon, the present analysis will focus on cyberterrorism; the extreme nature of this specific form should help in understanding more clearly the causes, the consequences and the potential remedies to all cyber threats.

To talk about cyberterrorism, it is necessary to start by discussing where terrorism is coming from. Most of the literature on terrorism and, most notably, General David Petraeus's *Manual on Counterinsurgency* (2006) converge on the fact that insurgents and terrorists belong to a single category: "rebels" who use a variety of techniques, depending on the circumstances.[17] Moreover, there is expert consensus on a few key characteristics. Terrorists have political or ideological objectives. They are "non - state actors", not part of conventional governments. Their intention is to intimidate an audience larger than their immediate victims, in the hope of generating widespread panic and often, a response from the enemy so brutal that it ends up backfiring by creating sympathy for the terrorist's cause. Their targets are often ordinary civilians, and, even when terrorists are trying to kill soldiers, their attacks often don't take place on the field of battle. Consequently, the terrorists are rational actors. Robert Pape a political scientist at the University of Chicago, built a database of three hundred and fifteen suicide attacks between 1980 and 2003, and drew a clear conclusion: "What nearly all suicide terrorist attacks have in common is a specific secular and strategic goal: to compel modern democracies to withdraw military forces from territory that the terrorists consider to be their homeland." As he wrote, what terrorists want is "to change policy," often the policy of a faraway major powers. Pape asserts that "offensive military action rarely works" against terrorism, so in his view, the solution to the problem of terrorism could not be simpler: withdraw. Pape's "nationalist theory of suicide terrorism" applies not just to Hamas and Hezbollah but also to Al Quaeda; its real goal, he says, is the removal of the U.S. military from the Arabian Peninsula and other Muslim countries. Pape thinks of terrorists as being motivated by policy and strategic concerns.[18]

By contrast, Mark Moyar dismisses the idea that "people's economic grievances" are the main cause of popular insurgencies.[19] He regards anti-insurgent campaigns as "contest between elites". Of the many historical examples he offers, the best known is L. Paul Bremer's de-Baathification of Iraq, in the spring of 2003 in which the entire authority structure of Iraq was disbanded at a stroke, creating the basis for a terrorist campaign against the American occupiers. One of Moyar's chapters is about the violent American South during Reconstruction. Rather than

[17] See also O'Neill, *Insurgency*.
[18] Pape, *Dying*.
[19] Moyar, *A Question*.

disempowering the former Confederates and empowering the freed slaves, according to Moyar, the victorious Union should have maintained order by leaving the more cooperative elements of the slaveholding. Effective counterinsurgency, he says, entails selecting the élites you can work with and co-opting them.

Audrey K. Cronin shares Pape's view that most terrorists are people who want control of land. The odds are against them, because of their lack of access to ordinary military power and other resources, but, if they do succeed, they can be counted upon to try to ascend the ladder of legitimacy and to some kind of governing status (for instance, the I.R.A. in Northern Ireland and the Palestine Liberation Organization in the West Bank and Gaza).[20]

Cronin goes through an elaborate list of techniques for hastening the end of a terrorist campaign. She believes, for instance, that jailing the head of a terrorist organization is a more effective counter-measure than killing him. Negotiating with terrorists can work in the long term, Cronin says, not because it is likely to produce a peace treaty but because it enables a state to gain intelligence about its opponents, exploit differences and separate factions.

In his work, Eli Bernman stresses the social services that terrorist groups provide to their members.[21] Bernam's book applies to terrorism the ideas of a 1994 article by the economist Laurence Iannaccone, called "Why Strict Churches Are Strong" (*AJS* Volume 99 Number 5, March 1994, 1180-1211). Iannaccone explains that strict religions function as economic clubs. They have appeal because they are able to offer benefits and this involves high "defection constraints." Berman's main examples are Hezbollah and the Taliban whom he calls "some of the most accomplished rebels of modern times". These organizations provide help and services in area where there is much need. Their members do not defect because they will be treated brutally if they do it and live in areas with no opportunity of change. According to Bernman, the use of suicide bombing is an indication not of the fanaticism or desperation of the individual bomber (most suicide bombers are not miserably poor and alienated adolescents) but of the high cohesion of the group.

The idea of treating terrorists as rational actors is embraced by General Petraeus; as he states in the *Introduction* of his 2006 Manual, soldiers and marines are expected "to be nation builders as well as warriors, to help re-establish institutions and local security forces, to assist in the rebuilding of infrastructure and basic services, and to facilitate the establishment of local governance and the rule of law". Petraeus has absorbed the theory that terrorist and insurgent groups are appeased by the provision of social services. His manual is devoted to elaborating ways in which counterterrorism must compete for people's loyalty by providing better services in the villages and

[20]Cronin, *How Terrorism*.
[21]Bernam, *Radical*.

encampments of the deep-rural Middle East. But this approach often does not work. Instead, helping people in areas where insurgents are well-established may help only the terrorists.

However, when terrorism meets information and communications technologies, it becomes cyberterrorism. According to General Petraeus: "… Interconnectedness and information technology are new aspects of this contemporary wave of insurgencies. Using the Internet, insurgents can now link virtually with allied groups throughout a state, a region, and even the entire world. Insurgents often join loose organizations with common objectives but different motivations and no central controlling body, which makes identifying leaders difficult … While the communications and technology used for this effort are often new and modern, the grievances and methods sustaining it are not."[22]

Box 1.1 describes the major cyberterrorist attacks as presented in the literature to date.

[22] Cf. Ibid., 4.

BOX 1.1 Cyberterrorist attacks

Terrorist use cyber space to cause disruption. Terrorists fight against governments for their cause, and they use every means possible to get what they want. Cyber-attacks come in two forms; one against data, the other, against control systems (Lemos, 2002). Theft and corruption of data leads to services being sabotaged and this is the most common form of Internet and computer attack.

In July 1997, the leader of a Chinese hacker group claimed to have temporarily disabled a Chinese satellite and announced he was forming a new global cracker organization to protest and disrupt Western investment in China. In September 1998, on the eve of Sweden's general election, saboteur defaced the Web site of Sweden's right-wing moderate's political party and created links to the home pages of the left-wing party and a pornography site. That same month, other saboteurs rewrote the home page of a Mexican government Internet site to protest what they said were instances of government corruption and censorship.
(See Curran et al. in Janczewski and Colarik, eds., *Cyber Warfare*, 1-6).

In 1998, a terrorist guerrilla organization flooded Sri Lankan embassies with 800 e-mails a day for a two-week period. The messages simply read "we are the internet Black Tigers and we're doing this to interrupt your communications." Intelligence departments characterized it as the first know attack by terrorists against a country's computer systems. Internet saboteurs defaced the home page of, and stole e-mail from, India's Bhabha Atomic Research Center in the summer of 1998. The three anonymous saboteurs claimed in an Internet interview to have been protesting recent Indian nuclear blasts (Briere, 2005).

Attacks which focus on control systems are used to disable or to manipulate physical infrastructure. This is what happened in an incident in Australia in March 2000 where a disgruntled employee (who failed to secure full-time employment) used the Internet to release 1 million liters of raw sewage into the river and coastal waters in Queensland (Lemos, 2002). Actually, it took him a total of 44 failed attempts to breach the system and his 45th attempt was successful. The first 44 were not detected

According to FBI reports of 2005, terrorists have used identity theft and credit card fraud to support activities by Al Qaeda cells. Also, according to press reports, Indonesian police officials believe that the 2002 terrorist bombings in Bali were partially funded through online credit cards fraud. Furthermore, The Internet is now used as a major tool for insurgents in Iraq: they have created many Arabic-language websites that contain code plans for attacks or that provide instructions on how to build and operate weapons and how to pass through border checkpoints. Furthermore, news articles report that the new generation of terrorists, such those behind the July 2005 bombings in London, are learning how to avoid detection by law enforcement computer technology (CRS 2007).

On July 2008, the San Francisco Chronicle reported that a 43 year old computer network administrator, held the city's Fiber WAN network hostage, creating a password that granted him exclusive access to the city's new Fiber WAN. The system contained records such as officials' email, city payrolls files, confidential law enforcement documents and jail inmate bookings. He was charged with four counts of computer tampering. The magazine says that he gave pass codes that did not work to police and refused to divulgate the true code, even when threatened with arrest. City officials said that his denial of access to other system administrators could cost millions of dollars (Van Derbeken Jaxon, "S.F. Officials Locked Out of Computer Network," *San Francisco Chronicle*, 15 July 2008, http://www.sfgate.com/bayarea/article/S-F-officials-locked-out-of-computer-network-3205200.php**)**.

Overall, many security experts agree that a cyber-attack would be most effective if it were used to amplify a conventional bombing. However, they disagree about whether a widespread coordinated cyber-attack by terrorists is a near- term or long term possibility. Terrorists may also be developing links with cybercriminals that will allow them to have access to high level computer skills. The time may be approaching when a cyber-attack may offer advantages that convince terrorists to attack (CRS, 2007).

2. The impact of Cyberterrorism

2.1 How do cyber warriors and cyberterrorists strike?

The physical forms of cyberterrorism, cyber warfare and cybercrime look very much alike but, to assess the impact of cyber-attacks, it is necessary to understand how these operations are carried out. These actions are managed using many technologies. However, the phases of a cyber-attack follow the same pattern as a traditional crime.[23] There are as follows:

- First, the attack starts with the *reconnaissance* of the intended victim. It requires observing the normal operations of a target to acquire basic information on the victim such as hardware and software used regular and periodic communications and format of correspondences.
- Second, the attack implements the *penetration* phase. Unless the attacker is inside a system, there is little that can be done to the target.
- Third, when the attacker is inside the system, *he tries to identify and expand the internal capabilities*, looking for access to the more restricted and higher value areas of a given system.
- Forth, *the intruder damages the system or steals selected data/or information.*
- Finally, *the attacker removes any evidence of a penetration*, theft and so forth, eliminating ant traces by editing or deleting log files.

In general, today cyber-attacks consist primarily of:

- *Malware*. According to the OECD, malware is "a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."[24]

  Malware includes malicious software code often referred to as "viruses", "worms" and "Trojans."

  ✓ Viruses have been available since the 1960s. Essentially, a computer virus is an "a self-replicating program that attaches itself to another program or file in order to reproduce.

[23] See Janzewski and Colarik, eds., *Cyber Warfare.*
[24] OECD 2009.

When a given file is used, the virus will reside in the memory of a computer system, attach itself to other files accessed or opened, and execute its code."[25]

- ✓ Worms are a "type of malicious software that does not need another file or program to replicate it, and as such, is a self-sustaining and running program. The primary difference between viruses and worms is that a virus replicates on a host system while a worm replicates over a network using standard protocols. Another use of worms that are less destructive and more subversive has been designed to monitor and collect server and traffic activities, and transmit this information back to its creator for intelligence and/or industrial espionage."[26]
- ✓ Trojans are "malicious programs that are intended to perform a legitimate function when it in fact also performs an unknown and/or unwanted activity. Many viruses and worms are delivered via a Trojan horse program to infect a targeted system, install monitoring software such as keyboard loggers (i.e. a program that records every keystroke performed by a user) or backdoors to remotely take control of the system, and/or conduct destructive activities on the infiltrated system."[27]

Malware attacks are delivered via email attachments, Web browser scripts and vulnerability exploit engines.

- *Denial of Service* (DoS) or distributed Denial of Service (DDoS) attacks. The United States Computer Emergency Readiness Team (US-CERT) classifies an incident as a DoS attack if it "successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS."

- *Unauthorized access* is a successful intrusion into an information system to gain logical or physical access without permission. According to the classification of the Computer Security Division of the National Institute of Standards and Technology (NIST) the following incidents are examples of unauthorized access: "An attacker runs an exploit tool to gain access to a server's password file" or "a perpetrator obtains unauthorized administrator level access to a system" (http://csrc.nist.gov/index.html). Targeted attacks fall in this category and exploit a maliciously crafted document or executable, which is emailed

[25] Ibid.
[26] Ibid.
[27] Ibid.

to a specific individual. These emails will be dressed up with social engineering elements to make it more interesting and relevant.

- *Advanced Persistent Threats* (APTs) are classified as an evolution of 'targeted attacks'. According to the *Symantec Internet Security Threat Report* (ISTR) 2013, they are designed to target a particular individual or organization. APTs are conceived to stay below the radar, and remain undetected for as long as possible (http://www.symantec.com/security_response/publications/threatreport.jsp).

- *Phishing* is the malicious means of acquiring user information, such as usernames and credit card details, through the use of websites or e-mails masquerading as those of a trustworthy entity.

The resources for attacking targets are non-static but evolve and improve over time; they are becoming more sophisticated and challenging. If technical progress can and should not be held back, technical progress applies to computer viruses as well. The OECD has rightly pointed out that continuous innovation and the increasingly openness of the network are forcing IT departments, IT security companies and law enforcement to keep pace with the actions of malicious users and malware technologies. Malware attacks remain the biggest Internet threat to all computer users, as fake anti-virus and search engine optimization poisoning have become commonplace. Furthermore, the introduction of new polymorphic viruses that use code modification or code encryption techniques are making the detection by anti-virus scanners more difficult.

This technical progress is not to be limited to the polymorphic viruses. The Virus Construction Kits make the work easier for the clueless virus writers, who did not themselves have the ability to create an encryption routine. Through the international networks these ready-made polymorphic routines were soon spread all over the world and made available to a wide audience.

Operation Aurora launched in 2011 was another example. This sophisticated and targeted attack focused on the intellectual property repositories of high-tech companies such as Adobe Systems, Google, 5 Juniper Networks and Rackspace. The primary goal of Operation Aurora was to gain access to and potentially modify intellectual property repositories in high-tech firms. Further analysis revealed that Operation Aurora used hosts primarily located in China, Germany, Chinese Taipei, the United Kingdom and the United States.[28]

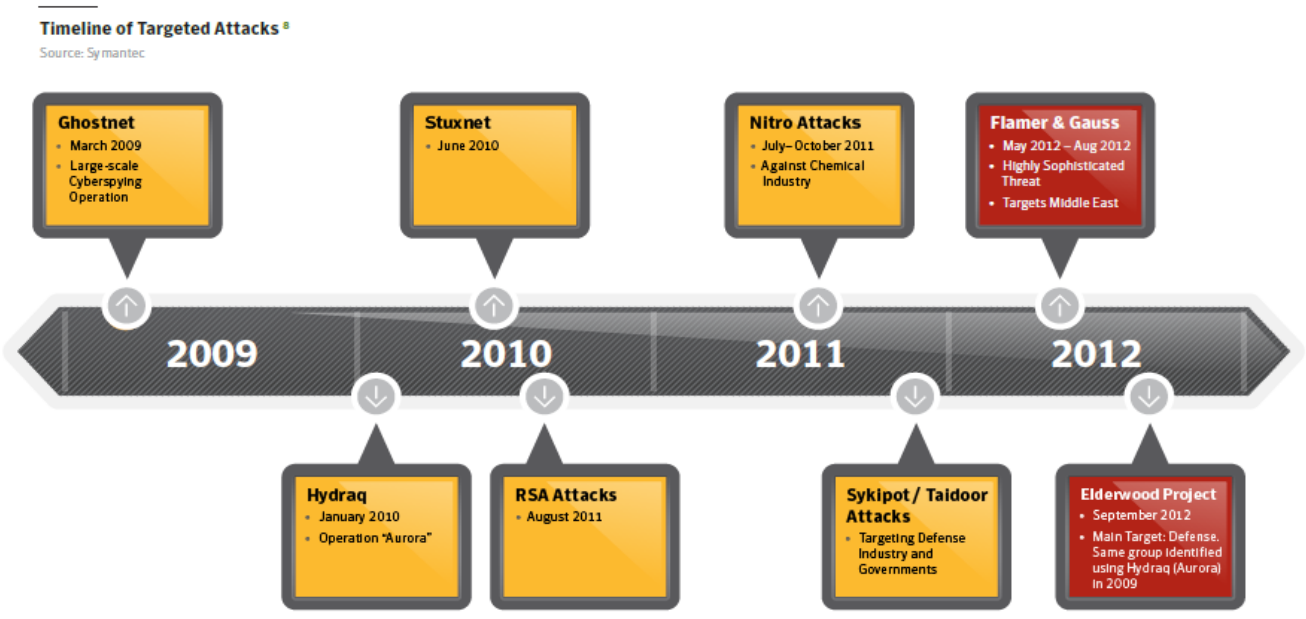
[28] OECD 2012, 6; "Protecting Your Critical Assets. Lessons Learned from "Operation Aurora," *McAfee White Paper*, http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

The goals of these attacks can be diverse. In some cases the objective is to show the vulnerability of the systems. In others, there are political statements about the entities that have been attacked. In others, the purpose is stealing information, intellectual property or intelligence.

The entity of the damages depends on the intention of the attacker. For instance, the APTs may include military, political or economic intelligence gathering, confidential or trade secret threat, disruption of operations, or even the destruction of equipment. To put it into the words of U.S. Secretary of Defense Leon Panetta: "Just as nuclear war was the strategic warfare of the industrial era, cyber warfare has become the strategic war of the information era."[29]

The same techniques used by cybercriminals may also be used by states and state proxies for cyber-attacks and political espionage. It is difficult to attribute a targeted attack to a specific group or a government without sufficient evidence. However, the motivation and the resources of the attacker sometimes suggest the possibility that the attacker could be state sponsored: these attacks appear to be rare in comparison with regular cybercrime, but have often gained notoriety. Figure 2.1 features the major targeted attacks from 2009 to 2012.

Figure 2.1. Timeline of Targeted Attacks



Source: *Internet Security Threat Report*, 2013

[29] *Aviation Week and Space Technology*, October 22, 2012, 82, http://www.aviationweek.com.

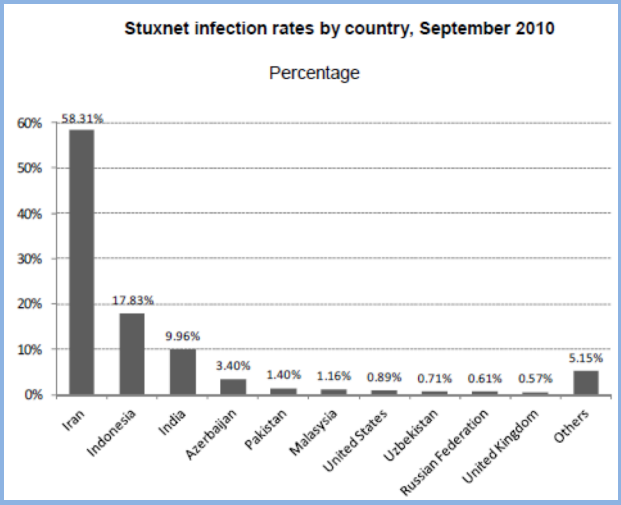
Stuxnet deserves a major attention as one of the state sponsored cyber-attack against Iran more relevant (see Box 2.1).

Box 2.1 Increasing sophistication of cyber security threats: the case of Stuxnet

No malware has attracted as much attention from security experts and the media as Stuxnet. Security experts described it as "groundbreaking", "incredible large and complex", and even "perfect from a technical point of view" (Falliere, Murch and Chien, 2011; Keizer, 2010; Matrosov et al., 2011). Some have also spoken of Stuxnet as a new generation "cyber weapon" (Langer, 2011). In any case, security experts agree that the following attributes make this malware special and contribute to its high level of sophistication:
Stuxnet exploits up to four zero-day Microsoft vulnerabilities, 6 an unprecedented number within a single malware. Two of these vulnerabilities have allowed Stuxnet to propagate undetected over multiple channels, namely over local area networks (LAN) and through removable drives.

- Stuxnet was built to target and compromise a very specific configured system, namely a supervisory control and data acquisition (SCADA) system controlled by a Siemens programmable logic control (PLC) software. These systems are often not even connected to the Internet (Falliere et al., 2011).
- Stuxnet uses up to two valid digital signatures making the infected systems believe the malware is legitimate.
- Stuxnet includes a built-in uninstall mechanism and an infection counter to enable it to self-destruct after it reaches a maximum number of infections. This results in a more controlled infection and minimizes the prevalence and as such the potential discovery of the malware.

As of September 2010, Symantec had counted approximately 100 000 Stuxnet infected hosts worldwide with Iran hardest hit (Figure 2.2). Security experts believe that this fact and the presence of a damage control to prevent uncontrolled infection increase the likelihood of Stuxnet having been designed and deployed explicitly to target SCADA systems in Iran.



Source: Falliere, Murch and Chien (2011)

Another indication of the high level of sophistication of Stuxnet is the amount of person-hours required to develop the malware. Security experts from Kasperky, Symantec and other firms estimate that it may have taken six to nine months and five to ten core developers to develop Stuxnet, "not counting numerous other individuals, such as quality assurance and management" (Falliere, Murch and Chien, 2011; Matrosov et al., 2011). Some experts further estimate the development cost of Stuxnet at around USD 3 million (Hesseldahl, 2010). Given the sophistication of Stuxnet and the knowledge required to successfully launch the attack, some security experts suggest that this type of attack would require resources only available at the level of a national government (Fildes, 2010; Halliday, 2010).

Source: OECD 2012

A recent report by a security firm Mandiant describes in great detail an example of cyber espionage activity funded and managed by the Chinese government against US and European targets (see Box 2.2 for details).

Box 2.2 Advanced Persistent Threats 1 (APT1): Exposing One of China's Cyber Espionage Units

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department ,which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.The nature of "Unit 61398's" work is considered by China to be a state secret; however, it is believed that it engages in harmful "Computer Network Operations."
Unit 61398 is partially situated on Datong Road in Gaoqiaozhe, which is located in the Pudong New Area of Shanghai. The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people. China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense. Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries. APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property. Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership. APT1 maintained access to victim networks for an average of 356 days. The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months. Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period. APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries. Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language. The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world. APT1 controls thousands of systems in support of their computer intrusion activities. In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109). In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators. We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers. Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors. APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

Source: M-Trends 2013: *Attack the Security Gap*, 2013

Overall, the last few years have registered increasingly sophisticated and widespread use of cyber attacks. In the near future, cyber-attacks will continue to be a way for tensions between states to play out. Furthermore, in addition to state-sponsored activities, non-state sponsored attacks, such as attacks by nationalist activists against those whom they consider to be acting against their country's interest, will continue.

2.2 What is the scale of these strikes?

The scale and effects vary among users, consumers or business but they are becoming more and more pervasive due to the ability of the attackers to use the most common applications and the most used websites.

Figures 2.3 a and b present the results of the Norton Survey, run by Symantec, on Consumer Cybercrime in 24 countries (Australia, Brazil, Canada, China, Colombia, Denmark, France, Germany, India, Italy, Japan, Mexico, Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, South Africa, Sweden, Turkey, United Arab Emirates, United Kingdom, Unites States of America) involving 13,018 adults aged 18-64.

It is striking to discover that a population greater than the European Union, 556 million citizens, is victimized every year by cybercrime: 1.5 million people per day, 18 victims per second! Furthermore, what it is more interesting is that **cybercrime is changing face, going mobile and going social!** As 2 out of 3 adults use a mobile device to access the Internet, mobile vulnerabilities doubled in 2011 from 2010. At the same time, 4 out of 10 social network users have fallen victim to cybercrime on social networking platforms in 2011.

Fig. 2.3 a Consumer Cybercrime

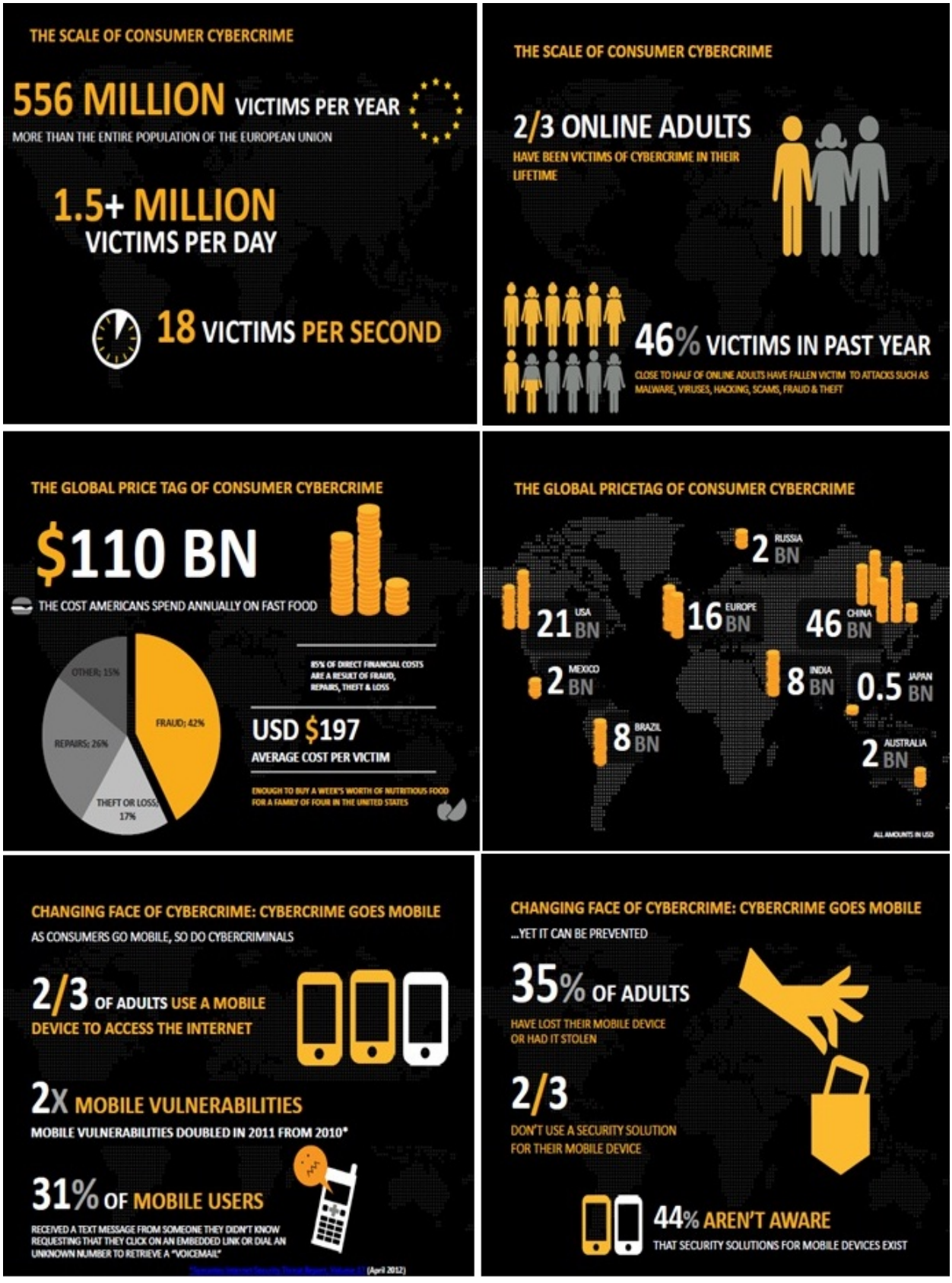
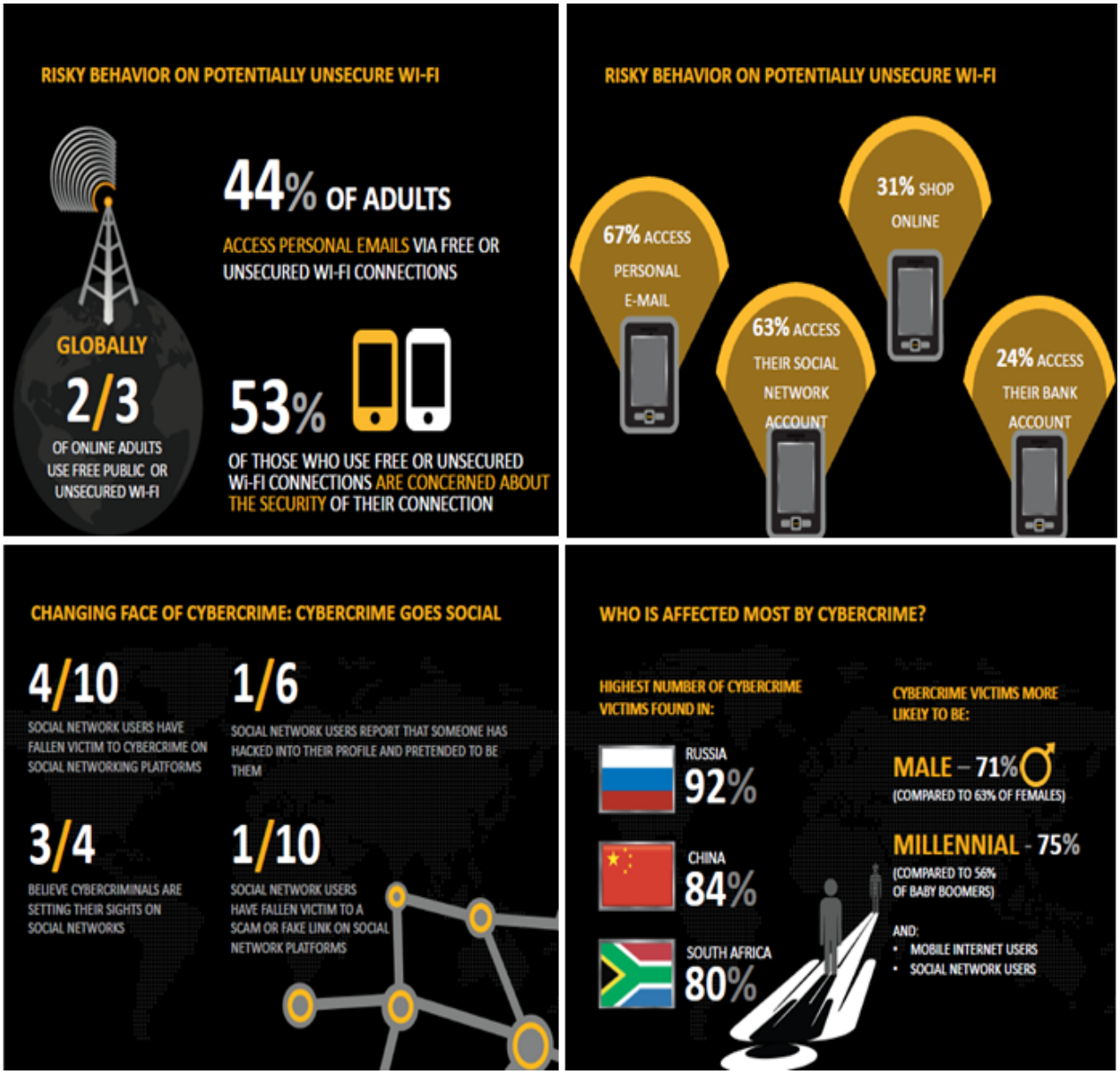


Fig. 2.3 b Consumer Cybercrime

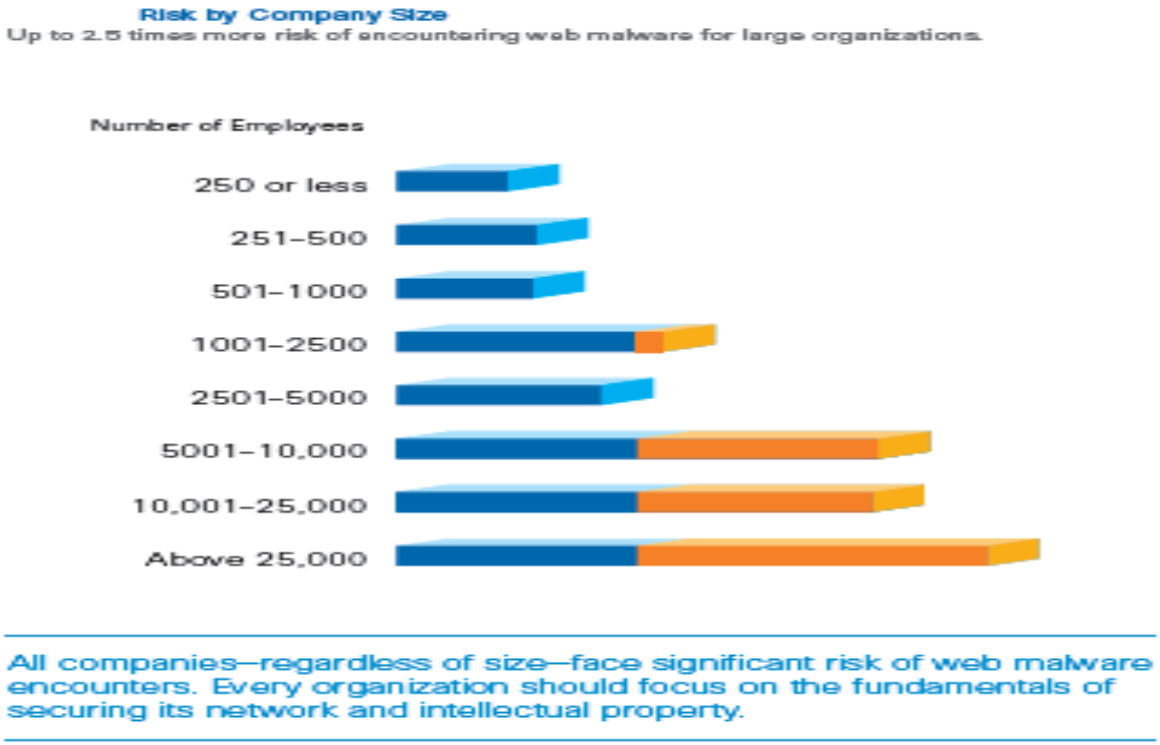


Looking at malware, it is interesting to discover that **the web is an equal opportunity infector!** Web malware is available everywhere people visit the Internet including the most legitimate websites such as those visited for business purposes. A Cisco Report shows that, regardless of size, all companies face significant risk of web malware. Largest enterprises (25,000+ employees) have more than 2.5 times the risk of being infected by malware than smaller companies.[30]

This increased risk can be explained by the higher intellectual property assets that bigger companies have and thus are more frequently targeted. (See Figure 2.4).

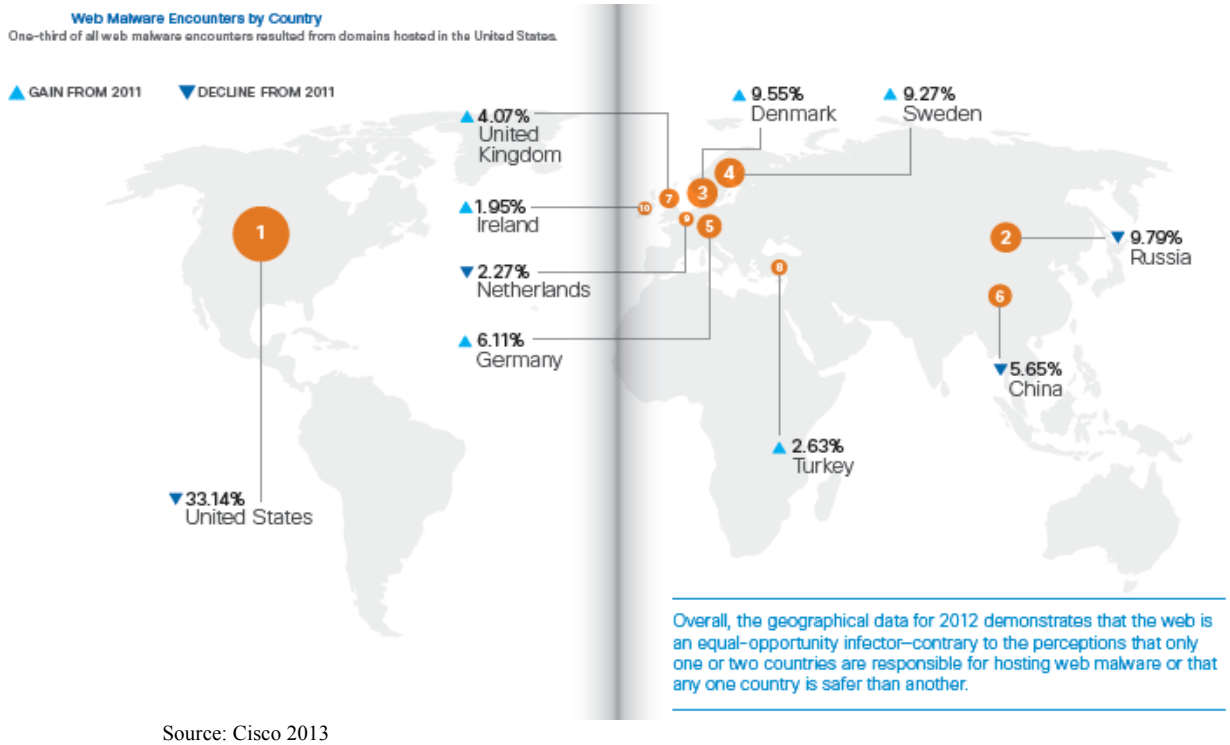
[30] Cisco, *Report* 2013.

Fig. 2.4: **Risk by Company Size**



The geographical data of malware distribution in 2012 (see Figure 2.5) shows that malware is hosted all over the world. The United States keeps the top ranking in 2012 with 33% of all web malware encounters occurring via websites hosted in the United States.

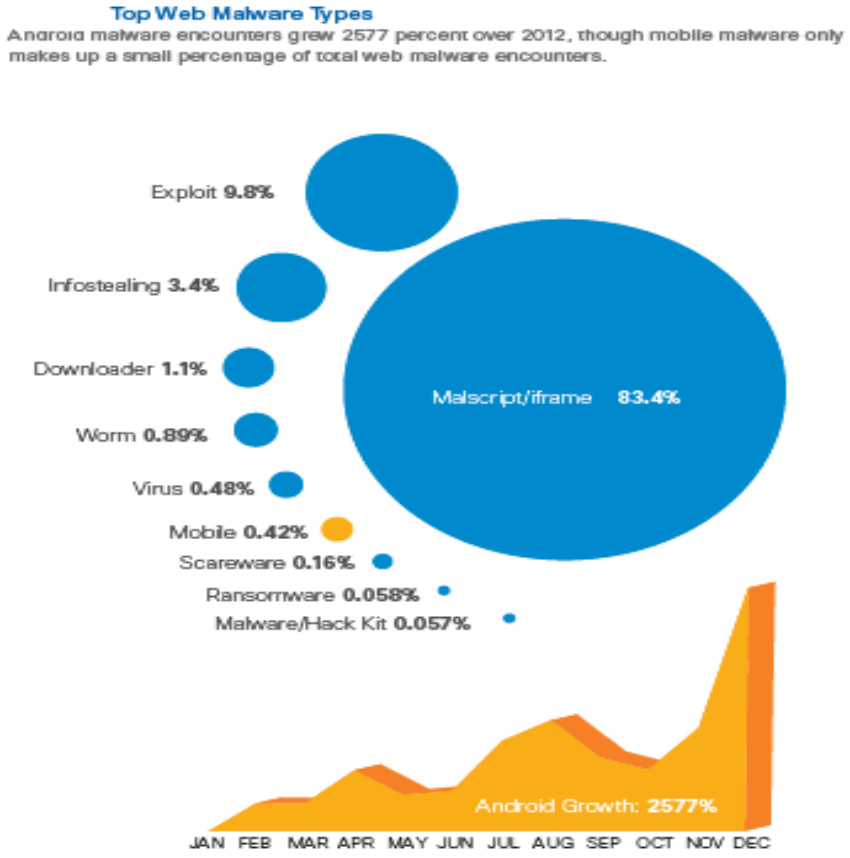
Figure 2.5: Web Malware Encounters by Country



Source: Cisco 2013

Figure 2.6 analyzes malware type in 2012; it shows that Android malware grew much faster than any other type of web malware.

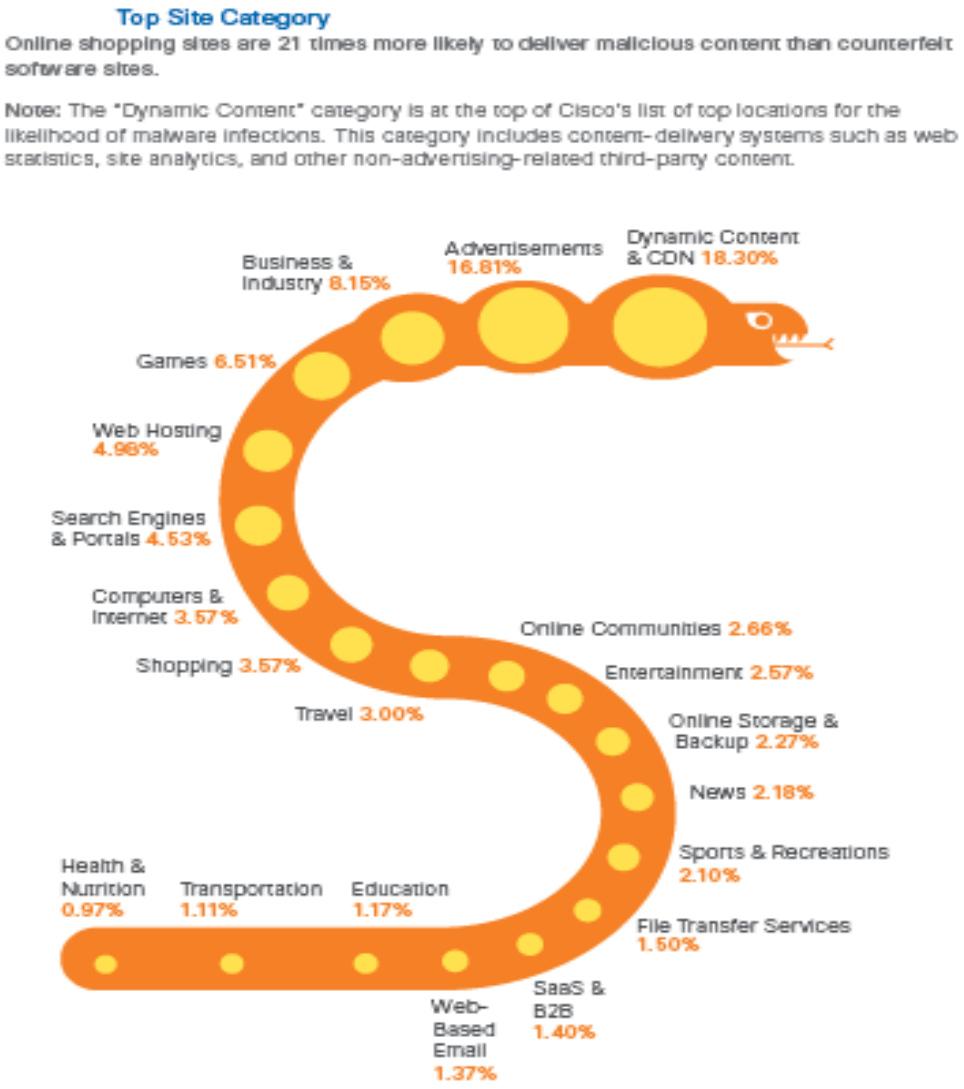
Figure 2.6: Top Web Malware Types



Source: Cisco 2013

However, it is important to note that mobile malware accounts for only 0.5% of overall malware, with Android taking over 95% of all mobile malware encounters. Looking at the full picture of malware types, malicious scripts and iFrames covered 83% of encounters in 2012. Exploits follow with 9.8% of encounters. The idea that malware infections usually result from "risky" sites such as counterfeit software is a misconception. Cisco's analysis shows that the majority of infections happen browsing mainstream websites. Figure 2.7 shows this result very clearly. Dynamic content web sites (web statistics, site analytics, and so on) have the highest likelihood of malware infections (18, 30%). Advertisements, business & industry and games sites follow with respectively 16, 81 %, 8, 15% and 6, 51 % likelihood of infections.

Figure 2.7 Top Site Category



Source: Cisco 2013

According to Websense,[31] malware infections and data theft were increased last year by emails. "Only one in five emails was safe or legitimate and in a blind phishing study, Websense found that more than 50 percent of users accessed email from outside corporate network, [...] beyond the reach of traditional defenses". Furthermore, cybercriminals are increasingly using **spear-phishing** techniques. These attacks begin with a cybercriminal performing online "reconnaissance" of a targeted victim's work, interests, and education. This information allows the cybercriminal to create personalized messages that entice the victim to click on a link or provide important information, without generate suspicion. Phishing hosts shift frequently worldwide and may even change in the middle of an attack in response to potential detections. They may also use more than one host to send the most email in the shortest time (Fig. 2.8). Two thirds of phishing

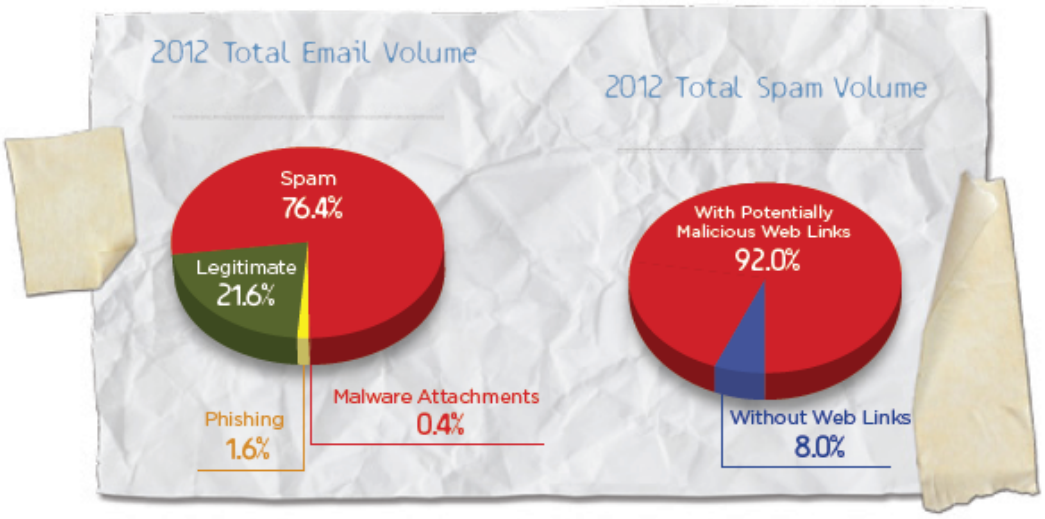
[31] Websense, *Threat Report*, 24-26.

emails were sent on Mondays or Fridays, when people are more distracted by personal matters. Furthermore, scheduled events, such as big sport events or special holidays offer opportunities for abuse by cybercriminals that use fake offers to capture victim's attention.

Figure 2.8

As shown in Figure 2.9, Websense also recalls that global spam grew in 2012 to 76% of all email volume, reaching more than a quarter of million emails sent per hour. However, spam is no longer a nuisance! Last year, 92% of email contained web links pointing to phishing, malware or other dangerous content.

Figure 2.9

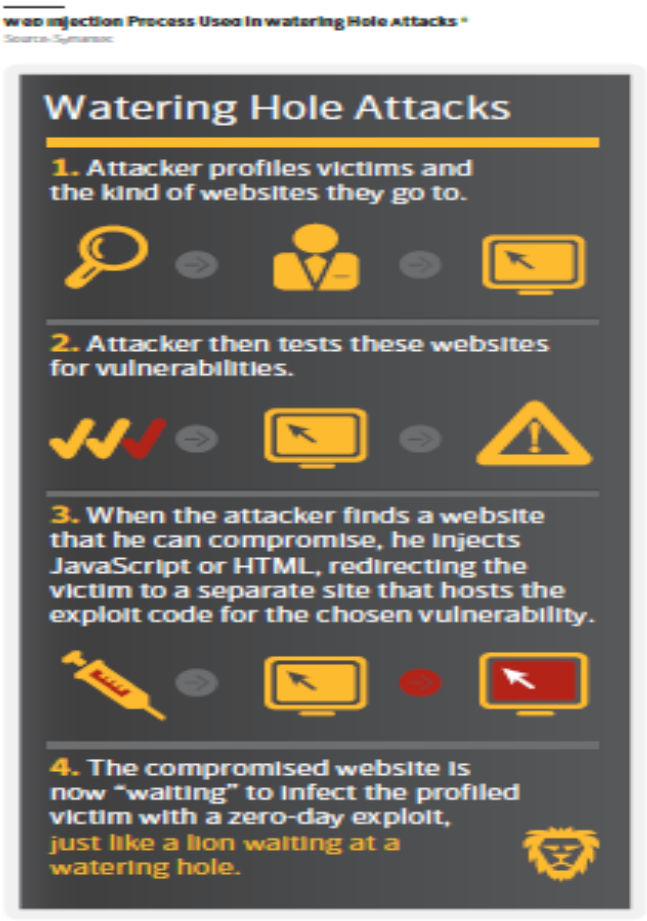


Targeted attacks, sometime also called APTs, are becoming of increasing concern. According to recent research from Quocirca (February 2013), across 100 medium to large organizations in the UK, over 70% admitted to having been victim of a targeted attack. More exactly, the United Kingdom confronts an attack from up to 70 sophisticated cyber espionage operations every month against its government and industry networks. Symantec (2013) estimates the global average of targeted attack worldwide in 116 a day.

According to another study by the Ponemon Institute (February 2012), an alarming 67% of organizations believe that their current security measures are not good enough to stop such attacks.

As described in Figure 2.10, these attacks usually start in the form of spear-phishing email. Fancy social engineering techniques or "watering hole attacks" will induce employees to open malicious attachments or click on a malicious link, thus exploiting a zero day or unpatched vulnerabilities. Once inside, the malware will enable the cybercriminals to communicate with that device from outside. This type of attacks often stays under the radar of conventional detection tools for month or years. According to Verizon Report (2012), 83% of all business that discovered targeted attacks, did so after weeks or months since infection. The majority, 54% of businesses took months to discover the malware.

Figure 2.10



Source: Symantec 2013

In this context, it is helpful to mention that in September 2012, the FBI issued a warning to financial institutions that some DDoS attacks are carried out as a "distraction". While the hackers attempted to break into company's networks using different techniques, the DDoS was used to divert companies' IT staff attention towards the DDoS.

2.3 What is the economic impact of these strikes?

The size and the effects of these strikes are relevant. Quantifying their economic impact is quite a complex task due to the limited ability to measure the costs and the probability of cyber-attacks. There are no standard methodologies for cost measurement and the analysis of the probability of cyber-attacks is hindered by the reluctant behavior of organizations to make publicly available their own information on security breaches.[32] There are many reasons to explain this behavior:

- *Financial market impacts*. Stock and credit markets may react negatively to security breach announcements, increasing the cost of capital to reporting firms for being now perceived to be more risky than previously thought.
- *Reputation or confidence effects.* Negative publicity may effect firm's reputation or brand, generating loss of confidence from consumers and giving competitors competitive advantages.
- *Litigation concerns.* When a firm reports a security breach, investors, customers may use the courts to seek recovery of damages. Furthermore, if there is a track record of breaches, plaintiff may claim a pattern of negligence against the firm.
- *Liability concerns.* Officials of a firm or organization may be subject to sanctions if they do not comply with regulations that establish ad hoc standards for safeguarding customers and patient records.
- *Signal to attackers.* Admitting publicly the breach may alert hackers that an organization's cyber defense is weak and suggest further attacks.
- *Job security.* IT personnel may fear for their jobs after an incident and try to hide the breach from senior management.

The costs of this disclosure can be significant, while the benefits of improved disclosure – more efficacy and cost savings in security, usually are slow to arrive and benefit all firms (including

[32] This section is based on Cashell et al., *The Economic Impact of Cyber-Attacks*.

competitors). The unbalance between costs (sustained by a firm) and benefits (occurring to all) generates a market failure. Therefore, to encourage information sharing a stimulus from the government is required. In some countries, like the US, the government promotes public/private partnership to share security information, such as the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) survey. However the results, in terms of participation to these initiatives have been mixed.

2.3.1 *Estimated loss from cybercrime*

Several security consulting companies, such as Symantec, Cisco, Websense, run surveys and produce estimates of the costs and the losses due to cybercrime activities. Table 1 summarizes the most recent results clustered by consumer and business sectors. The estimates run from $1 trillion as overall impact, to $100,000 as average loss for an individual firm. Overall, the values vary significantly but are all quite relevant!

Table 1 Economic Loss from Cybercrime

PLAYER	Available data	IMPACT	SOURCE
Overall	President's Obama Declaration	$ 1 Trillion lost to Cybercrime	The Economist, July 2010
Consumer Cyber Crime	Total loss	$ 110 Billion	2012, Norton Cybercrime Report
	Average cost per victim	$ 197	
Business Cyber Crime	Average cost	$ 591,780	2012, Pomenon Institute
	Only 2 cases out of 77 Very large losses	 $20 million $25 million	2010/2011 CSI Computer Crime and Security Survey
	In general Average loss	below $100,000 per Respondent	

However, survey responses may be considered extremely subjective. Therefore, it may be worthwhile to look for a more objective measure of the effect of cyber-attacks on individual firms.

2.3.2 *Effect of cyber-attacks on stock prices*

One approach suggested in the literature, is to study the effect of attacks on stock prices. The price of a company's stock, in theory, is determined by the present value of the cash flows

expected from the firm's ouput. This value generates the wealth of the stockholder. Any event that modifies investor's expectations about the future stream of revenues is likely to affect the price of the stock.

By all means, some firms will be more exposed to cyber-attacks than others and the company's size plays a significant role. However what will probably make a difference is the different level of dependence on computer networks in conducting their business that characterizes some firms compared to others.

Traditional "brick and mortar" firms will be the least exposed to cyber-attack, compared to "clik and mortar" that conduct their business both on and off line, or internet firms that conduct their business exclusively on line. Furthermore, the extent to which a firm is affected might reasonably be linked to the type of attack. Denial of service (DoS) attack causes a temporary interruption of the company's capabilities of running their business. Instead security breaches are the ones that have the most lasting effects on the targeted firm, because they imply the theft or destruction of data.

Therefore, other things being equal, the more the firm depends on the Internet and the more intrusive is the attack, the more likely it is to generate significant financial impact on the firm. Table 2, summarizes these results.

Table 2

Potential Financial Consequences of a Cyber-Attack

Type of Firm	Type of Attack	
	DoS	Security Breach
Conventional Brick and Mortar (e.g., Coca-Cola)	Lowest	
Click and Mortar (e.g., Barnes & Noble)		
Internet Firms (e.g. Amazon, Ebay)		Highest

Source : Cashell et al. 2004

According to some analysts, there was a significant decline in stock prices of targeted firms in the days immediately following the cyber-attack. The window of the analysis is restricted to the days immediately following the attack to avoid capturing the effects of other events not related to the attack.[33] Table 3 presents the summary findings of those stock market studies.

[33] Ibid. 6.

Table 3: Summary Findings of Stock Market Studies

Summary Findings of Stock Market Studies

	Does attack cause drop in stock price?	Does type of attack matter?
Cavusoglu, et. al.	-2.1% overall	no
Campbell, et. al.	significant modest decline	yes
Ettredge & Richardson	-5% (DoS only)	N.A.
Garg, et. al.	web site defacing: -1.1% DoS: -3.6% non financial info: -1.5% financial info: -15%	yes

Source: Cashell et al. 2004

How relevant are these drop in stock prices in dollar terms? At the end of 2003, the time of the majority of the analyses here reported, the average market capitalization for a firm listed on the New York Stock Exchange was about $4.4 billion and for a company listed on NASDAQ was $870 million. A 2.5 drop in market capitalization is equivalent to an average loss of about $88 million for the NYSE and about $ 17 million for a NASDAQ company.

In the contest of the analysis of cyberterrorism, it may be worthwhile to mention that the literature on the impact of exogenous shocks such as terrorist bombing on financial market values shows also negative effects. However, it is necessary to differentiate the impacts of large scale events such as 9/11 from impacts of protracted terrorism such as in Israel and Spain.[34] More exactly, Chen and Siems who study the impacts of terrorist bombing on the US capital market, show that these events produced no abnormal returns on the day of the attack. The only exception was the event of 9/11 that, even after 6 trading days kept showing negative cumulative abnormal returns. [35] They conclude that the limited shock of the financial market is largely due to the increased resilience of the US capital market to exogenous shocks.

On the other hand, Eldor and Melnick[36] studying the impact of terrorism on the Israeli's capital market, show that protracted events in smaller market can have significant impacts and that the Israeli-Palestinian conflict reduced significantly the stock market capitalization. A similar result

[34] See Scheider et al., *The Economics of Terrorism and Counter-Terrorism*.

[35] Chen and Siems, "The Effects of Terrorism on Global Capital Markets." The terrorist attacks considered in the study include among others the bombing of Pan Am (December 21, 1998), the World Trade Center (February 26, 1993), Oklahoma City (April 19,1995), US Embassy Bombing in Kenya (7 August 1998).

[36] Eldor Rafi and Rafi Menlick, "Financial Markets and Terrorism."

is found by Abadie and Gardeazabal studying the relation between terrorism and stock market values in the case of the Basque country.[37]

2.3.3 *Insurance industry and cyber-attack risks*

In order to confirm the economic relevance of the impact of cyber-attacks, it is helpful to look at the way in which the insurance industry started to approach cyber-attack risks.[38] As these risks became larger and more common with the diffusion of the Internet, the reaction of the insurance industry followed two paths. First, they made clear that existing business insurance did not include coverage of cyber-risks. Second, they started to introduce ad hoc policies to cover these type risks that were not included in previous coverage packages. These policies vary a lot as to terms and coverage. The tendency is to avoid standard cyber-insurance policy. Policies can include both first and third party risks, with a greater preference for covering first third party risks. These policies cover the following risks: network security (damages due to direct attack), web content (copyright infringements), business interruption, cyber extortion and public image (the cost of repairing a company's reputation after a cyber-attack).

2.3.4 *Macroeconomic effects of cyber-attacks*

After looking at the economic impact of cyber-attacks at the firm level, it is helpful to complement this analysis studying the repercussion of cyber-attack on the economy as whole. In order to assess the macroeconomic effects of cyber-attacks on information systems, it is useful to recall that a substantial body of literature shows that the diffusion of computers and more in general of Information and Communications Technologies (ICTs) in the economy plays a significant role in increasing economic productivity and growth of a nation.[39]

There is broad evidence that the Internet and communications infrastructure is considered today a key platform to conduct business, connect people and provide government services. Therefore, any Internet services block or denial is creating big economic losses. Estimating the value of these losses can help to size the effects of cyber-attacks on the overall economy. However, it is necessary to mention that while a cyber-attack generally disable the target of an attack, more conventional physical attacks, such as bombing or natural disaster events, destroy the target of an attack.

Therefore, to capture the macro economic effects of cyber-attack, it is necessary to rely on real event of Internet block or denial. The events occurred in Egypt in 2001 represent a case in

[37] Abadie Alberto and Javier Gardeazabal, "The Economic Costs of Conflict."
[38] See Cashell et al., *The Economic Impact of Cyber-Attacks*.
[39] See: OECD 2003; OECD 2004; OECD 2008; LECG, *Economic Impact of Broadband*; Qiang and Rossotto, *Economic Impacts of Broadband*.

point. The Egyptian government has taken great steps in the past years to develop and promote the use and uptake of technologies. However, the shutdown of Internet and communications services for five days during the Arab Spring in February 2011 had a pronounced economic impact. According to the OECD, the direct costs could be estimated at minimum USD 90 million. "This amount refers to lost revenues due to blocked telecommunications and Internet services, which account for around USD 18 million per day, or, on a yearly scale, for roughly 3-4% of GDP. However, this amount does not include the secondary economic impacts which resulted from a loss of business in other sectors affected by the shutdown of communication services e.g. e-commerce, tourism and call centers. In fact, the IT services and outsourcing sector in Egypt has been a growing part of the economy and relies heavily on the Internet and communications networks. IT outsourcing firms in Egypt made USD 1 billion in revenues in 2010 (or around USD 3 million per working day), servicing overseas customers through call centers, helpdesks, etc. The longer term impact of the Internet and communications shutdown on Egypt's economy is hard to assess. The shutdown may impact negatively on foreign direct investment in the ICT sector and industries that rely on stable communications and the Internet. The loss of connectivity for five days to these vital business services could make them reconsider overall outsourcing plans. Attracting such firms has been a key strategy of the Egyptian government. Egypt has other sectors that depend on Internet and communications, notably a vibrant tourism sector. It is difficult to put a number to the loss of tourism due to the Internet shutdown alone, but it provides an idea of how much the Internet has become part of mainstream economic activities, even in Egypt. In regards to long-term effects, it may be extremely difficult to unravel the impact of the general political and social conditions from the shutdown of the Internet and mobile networks."[40]

2.4 What is the economic impact of cyberterrorism?

So far, it has been assumed that the physical forms of cyberterrorism, cyber warfare and cybercrime look very much alike and that the way in which all type of cyber-attack are carried out are quite similar. However, it reasonable to ask whether the final effects of cyberterrorism are to some extent different from other types of attacks, i.e. if the effects are more pervasive and can cause greater losses.

According to many experts, cyberterrorists will try to combine physical attacks with cyber-attacks.[41] Their action is very much focused on critical infrastructures: energy, transportation, telecommunications, water supply and waste management, agriculture and food supply, finance, public health, and essential government services. Hua and Bapna examined the potential threats of

[40] See OECD 2011.
[41] See Nakashima, " FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat."

cyberterrorism.[42] Their work draws on the analysis of Foltz[43] who summarized the major potential threats of cyberterrorism, as follows:

- Attack electrical power systems; gas and oil production, transportation and storage; water supply systems, banking and finance (Embar-Seddon);[44]
- Access a drug manufacturer's facility and alter its medication formulas to make them deadly (Wehde);[45]
- Access hospital records and change patient blood types (Gengler);[46]
- Report stolen information to others (e.g. troop movement) (Desouza and Hensgen);[47]
- Manipulate perception, opinion and the political and socioeconomic direction (Stanton);[48]
- Facilitate identity theft (Gordon and Ford).[49]

Compared to other forms of terrorism, cyberterrorism is more efficient since it requires fewer people and fewer inputs. Furthermore, cyberterrorists can act remotely and remain anonymous by using proxy servers and IP-change methods to hide their real addresses. For this reason, it is difficult for government's agents to trace and capture them.

Hua and Bapna developed a game theoretical approach in order to study the optimal information system security investment and compare the losses caused by cyberterrorists and common hackers.[50]

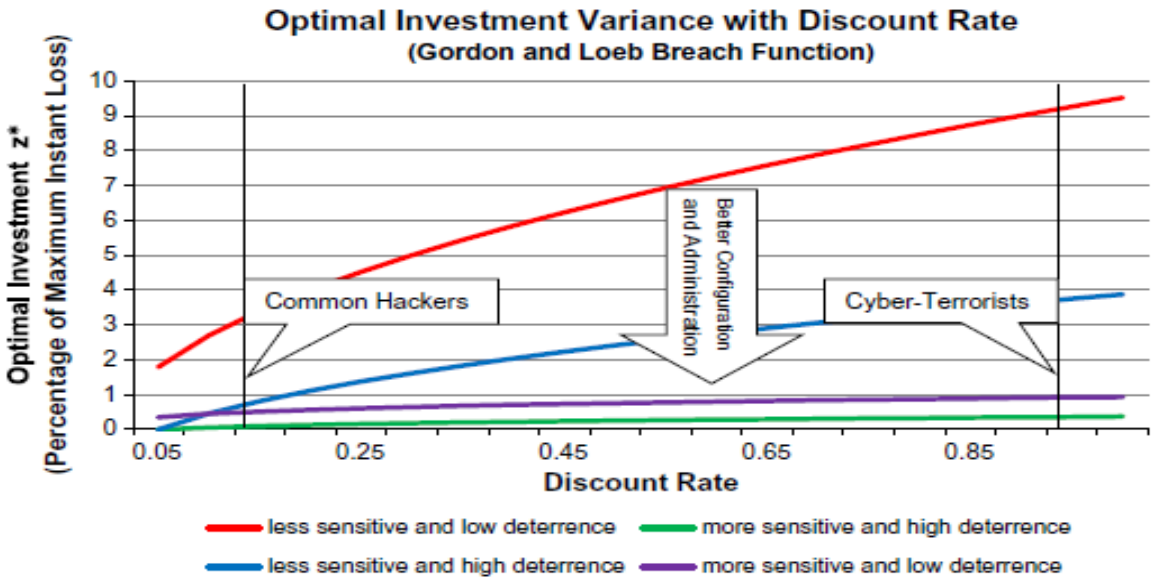
While cyberterrorists are a sub group of hackers, the most relevant difference between cyberterrorists and hackers relies in their motivation. Cyberterrorists are politically or religiously motivated. Generating terror among civilians and disrupting public and private infrastructure is their goal.

As shown in Fig 2.11, the authors consider different scenarios characterized by different values of the sensitivity of the breach function, of deterrence level and of the discount rate. "A sensitive breach function is a function where a moderate increase in the amount of investment in security can decrease breaching probability considerably" (the authors use a Gordon and Loeb

[42] Hua and Bapna, "The Economic Impact of Cyber Terrorism".
[43] Foltz, "Cyberterrorism, Computer Crime, and Reality."
[44] Embar-Seddon, "Cyberterrorism."
[45] Wehde, "US Vulnerable to Cyberterrorism."
[46] Gengler, "Politicians Speak Out on Cyberterrorism."
[47] Desouza and Hensgen, "Semiotic Emergent Framework."
[48] Stanton, Stanton, "Terror in Cyberspace."
[49] Gordon and Ford, " Cyberterrorism?."
[50] For an interesting survey on the use of game theory to study network security, see Manshaei & others, "Game Theory meets Network Security".

breach function).[51] Deterrence refers to the level of punishment for cyber attackers. "The punishment may include punishment of a person or a group or the party to which the lawbreakers belong. For cyberterrorism, the punishment may include anti-terrorism wars against the state where the cyberterrorists reside. Thus, for cyberterrorism the punishment may be more severe and in some cases exceed the losses caused to the victims". The discount rate is a proxy of the attacker's preference, where the preferences analyzed in the paper are cyberterrorism (high discount rate) and hacking by common hackers (low discount rate).

Figure 2.11



Optimal investment variance with discount rate changes (Gordon and Loeb Breach function).

Source: Hua & Bapna 2013

The game theory simulation model clearly shows that the optimal investments are far greater to protect Information System Security from cyberterrorist (high discount rate) than from common hackers (low discount rate). Therefore, "compared with common hackers, cyberterrorists are more dangerous. Common hackers prefer instant payoffs and act like shoplifters. They are opportunistic and cannot dedicate a long time to intruding into a single organization. Because common hackers are likely to cause less damage a lower level of security investment can deter them. However, if an organization is attractive to cyberterrorists because of the information it holds or its role in critical infrastructure, the Information System Security level should be higher."

[51] Gordon and Loeb, "The economics of information security investment."

3. The response to Cybercrime and Cyberterrorism

3.1 Cybersecurity as risk management

Given the variety of means and intensity of cybercrime described so far, what could be an optimal response to these threats and how can be properly designed? According to Anderson and Moore: "People have realized that security failure is caused at least as often by bad incentives as by bad design."[52] Players in the market decide the level of security they consider appropriate and rational, given their business models. Because security comes at cost, agents consider the cost and the benefits of accepting some level of insecurity.

The optimal level of cyber intrusions is not zero and the optimal level of cybersecurity expenditure is not infinity. Cybersecurity is a form of risk management; it corresponds to the willingness to master the risks linked to the use of information technologies and the costs generated by the protection of information systems from threats. "Security is never definitely achieved: the constant evolution of needs, systems threats and risks means that all security measures are potentially only temporary."[53]

Risk, vulnerability and threat are the key variables to be considered. The risk is defined as the danger that can be envisaged; it is quantified by the likelihood of damage and its resulting harm. The vulnerability is the weakness or the failure inherent in the environment (for instance information security infrastructure) in the absence of a control. The threat is the potential cause of undesirable event. A risk is then the product of the probability of an event based on the vulnerabilities and the threats that exist and the consequences of an incident:

$$\text{Risk} = (\text{Vulnerability, Threat, Impact})$$

The main steps for managing information risks are the following:

- identification of assets, based on security criteria;
- analysis of the vulnerabilities that characterize these assets;
- understanding of the threats (identification of their origins, of the motivations and scope to be exploited and of the amplifying factors);
- understanding of the risk (a matrix of probabilities and impacts);
- definition of counter-measures concerning the processes, the technology and the users.

[52] Anderson & Moore , *The Economics*, 610
[53] See Ghernaouti , *Cyber Power*, 361. Most of this section draws from Ghernaouti (2013)

Understanding the threats is one of the most critical issue of this process and also the one that has attracted the focus of the industry the most. As the number of threats discovered each year has sky rocked, the idea of being able to neutralize each threat has lost effectiveness. Therefore, the industry has been searching for a methodology to narrow down threats in a practical manner that allows efforts prioritization and optimal resources management.

Identifying which types of attacks are possible is only the first step. The most critical information is understanding which attacks are most likely to occur. Intel Information Technology Security has developed the *Treat Agent Risk Assessment* (TARA) that identifies the most likely attack vectors to support the development of optimal security strategies.[54] TARA methodology identifies which threat agents pose the greatest risk, their motivation, methods and objectives and how they map to existing controls, not on the weak points themselves.

The TARA methodology is based on three tools:

- Threat Agent Library (TAL)
- Common Exposure Library (CEL)
- Methods And Objectives Library (MOL)

[54] See INTEL (2007) and INTEL (2009).

The *Threat Agent Library*, defines a taxonomy of threat agents, based on eight common attributes, such as intent-hostile or non-hostile and access-internal or external. Using some unique combinations of these attributes, the TAL identifies 22 unique types of threat agents, such as reckless employee, competitor, terrorist, and others as shown in Table 4.

Table 4: Current Library of Threat Agents and Their Defining Attributes

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal	■	■	■						■		■	■							■		■
	External				■	■	■	■	■		■			■	■	■	■	■	■		■	
Outcome (1-2)	Acquisition/Theft												■			■				■		
	Business Advantage						■	■	■			■			■							■
	Damage	■	■	■	■					■	■			■			■	■	■		■	
	Embarrassment	■	■	■		■				■	■			■	■		■	■				
	Tech Advantage						■	■	■			■	■									■
Limits (max)	Code of Conduct		■	■																		
	Legal	■													■							■
	Extra-legal, minor					■	■	■	■				■				■	■		■	■	
	Extra-legal, major				■					■	■	■		■		■			■			
Resources (max)	Individual	■	■	■						■				■						■		
	Club				■													■				
	Contest																				■	
	Team								■													■
	Organization					■	■						■		■	■	■		■			
	Government							■			■	■										
Skills (max)	None				■									■						■		
	Minimal		■															■				
	Operational			■						■											■	■
	Adept	■				■	■	■	■		■	■	■		■	■	■		■			
Objective (1 or more)	Copy					■	■		■			■	■		■							■
	Deny							■			■											
	Destroy				■					■	■								■			
	Damage									■	■								■			
	Take														■	■			■	■		
	All of the Above/ Don't Care	■	■	■										■			■	■			■	
Visibility (min)	Overt		■		■			■							■		■	■				
	Covert	■				■										■			■		■	
	Clandestine			■			■		■			■	■							■		■
	Multiple/Don't Care									■	■			■								

Source: Intel IT Threat Assessment Group, 2007

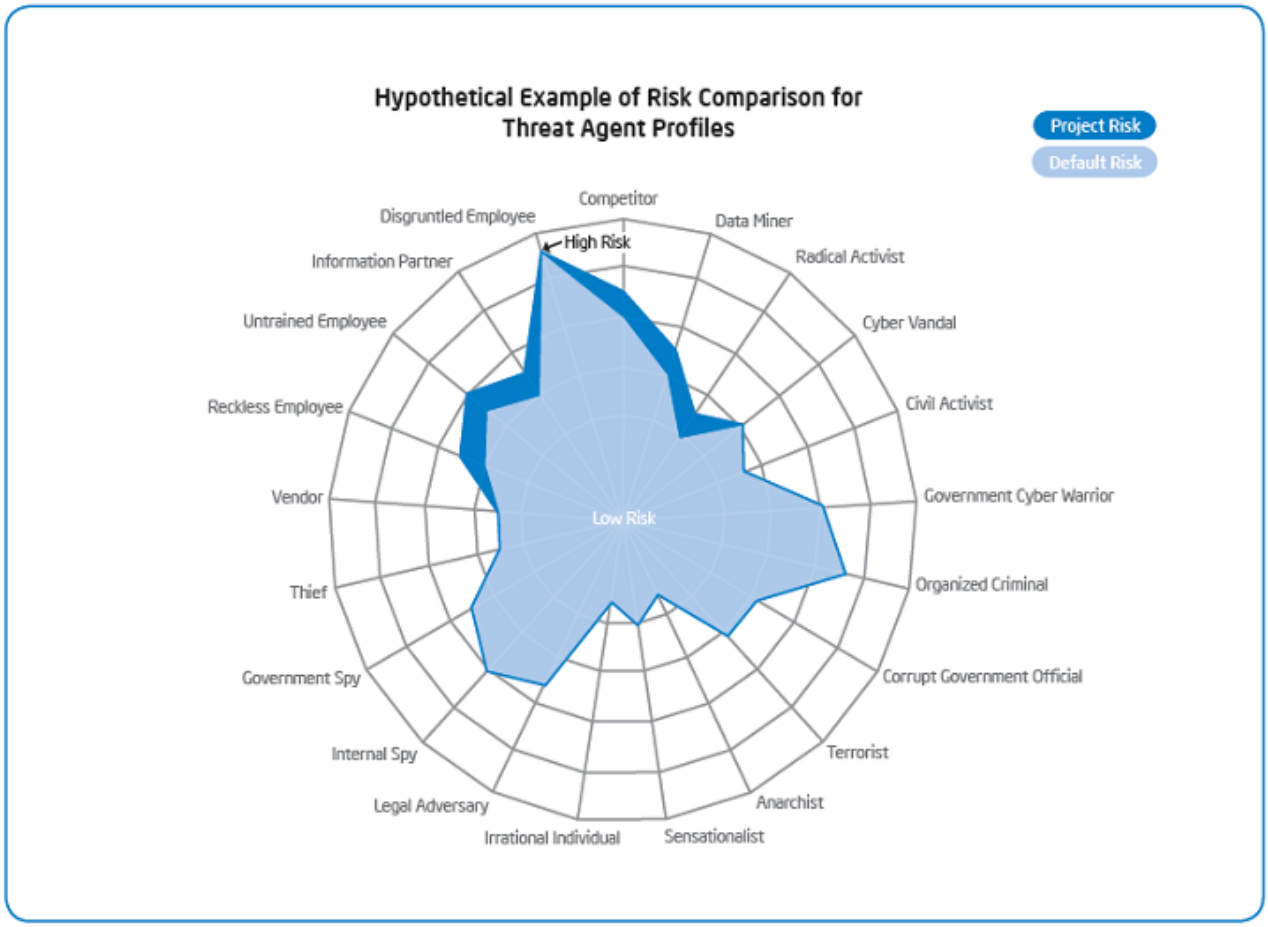
The description and rating of threat agents are refined and updated by a company's cross-functional team using his own experience and outside references and expertise. This detailed effort allows to identify in a useful way potential threat. For instance, instead of just using the "hacker" profile, the library specifies if the threat is coming from a "cyber vandal" (interested in system intrusions for prestige among peers) or from a "Data Miner," "Mobster," "Government Spy and Government Cyberwarrior."

The Common Exposure Library (CELs) collects known information security vulnerabilities and exposure – vulnerability without control- at Intel and from publicly available CELs. The CEL maps the vulnerabilities against current controls - processes and measure carried out to reduce the

risk of loss due to vulnerability- to show which exposures are residual. For instance, currently known viruses for the presence of antivirus, can be considered not an exposure.

The Methods and Objectives Library (MOL), describes known threat agent objectives –what are their goals and the most likely methods they will use to reach them. When the MOL is associated with the TAL, a picture of possible and likely attacks emerges, using many elements such as resources, objectives, typical methods and preferred vulnerabilities. Finally, when this emerging picture is completed with CELs information, it is possible to drop those vulnerabilities with sufficient controls while the residual vectors of attack emerge as the most critical area to manage. As shown in Figure 3.1 comparing the default risk of a very large project with projected risk using the TARA methodology, it is possible to derive the highest priority residual exposures. For instance, "irrational individuals" do not represent a major threat during this specific project, while "disgruntled employees " represent the highest risks.

Figure 3.1: The TARA methodology provides information on project specific information security risks, which may differ from an organization's default level of information security risks



Source: Intel, Prioritizing Information Security Risks

3.2 An efficient level of cybersecurity

Once the risks have been assessed, the objective of information security and of counter measures to fight cybercrime it is not to make money but to avoid losing it as an effect of a security accident that generated either direct financial losses or indirect harm. In this context, becomes necessary to estimates the cost of security in terms of budgets, products and training.

From an economic standpoint, the optimal result is not to prevent all attacks but to have an efficient level of attacks. Suppose that the expected cost for society from a cyber-attack – its cost discounted for the probability that the attack will occur - is 4 billion euro then, the efficient outcome for the society would be to invests up to 4 billion euro in cybersecurity to prevent the attack. Any additional expenses would not be justified because the cost of preventing the attack would be greater than the security gains.

Therefore, organizations and individual should invest appropriately in information security with the purpose of protecting their critical information infrastructures. Given the increasing role of cybercriminality, the best response is to be ready to face the information risks that have criminal origin. It is not if but only when is going to happen. The risk assessment process will help in prioritizing the security activities.

However, in this context, a critical question is: are individual firms, and society as whole investing the right amount in cyberdefense? In particular, because the protection against cyberterrorism implies protection of critical infrastructures, mostly owned by the private sector, it is reasonable to ask: do private players have sufficient capabilities and incentives to invest appropriately in cybersecurity or is government intervention required?

Very little empirical data exist on this issue. Studies from computer security firms, such as McAfee, suggest low level of investments from the private sector.[55]

According to Natan Sales,[56] whether a company is making socially optimal investments in cybersecurity and consequently who should pay for that company's cyberdefense, is a function of two related questions:

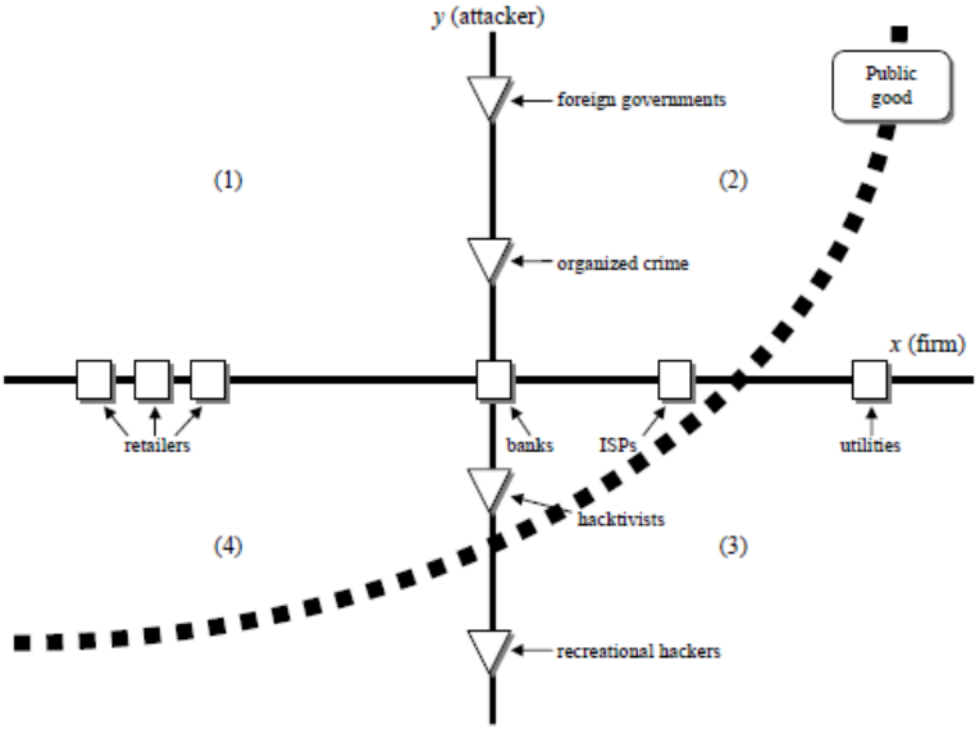
a) **What is the defending firm**? A company in a competitive market, an operator of a critical infrastructure or something in the middle?
b) **Who is the anticipated attacker**? Is it a recreational hacker, a foreign secret service or something else?

[55] See McAfee (2011), 13
[56] Sales, *Regulating Cybersecurity*, 8.

Figure 3.2 presents the range of possibilities. The x-axis describes the firms that might be attacked, ordered from left to right accordingly to the increasing social harms that a cyber-attack could generate. On the far left, there are firms in competitive markets where disappointed consumers could switch easily to other companies. An example would be online retailers such as Amazon. To the right there are financial institutions such as banks. The attacks to these institutions could be very disruptive, but these markets are quite competitive and consumers could move their account to other financial institutions. Then, there are the Internet Service Providers, where a successful attack could be quite harmful for the overall economy. Furthermore these markets are less competitive than the online retailing market. At the far right are power companies and other utilities. In this case the effects of cyber-attacks could be devastating: think about an attack to the power grids or to the turbines systems as Stuxnet did in Iran. Furthermore, utility markets are not competitive.

The y axis describes the attackers arranged from bottom to top according to their increased sophistication: at the bottom there are "recreational hackers", then "hacktivists" such as those from "Anonymous group". Further up, are organized crime syndicates, such those operating from Russia. Cyberterrorists can also be placed in this group.

Figure 3.2



Source : Sales, *Regulating Cybersecurity*

At the top, there are foreign governments' militaries and secret services. These are generally the most sophisticated attackers. State led cyber attackers from China, which are more active in stealing intellectual property rights, can also be included here.

The dotted curve predicts the combinations of victims and attackers that are likely to happen. Quadrant (4) is characterized by high frequency, low severity attacks: retailers could expect to be the target of frequent attacks from unsophisticated and a bit more sophisticated attackers. Quadrant (2) describes attacks that are low frequency but high severity: these are the attacks coming from foreign intelligence services, cyberterrorists and organized crime syndicates and will involve ISPs and public utilities. These attacks should be more rare but should be very devastating.

Quadrants (1) and (3), describe attacks less likely to happen because less attractive to potentials attackers. In quadrant (1), foreign service has no incentives to attack retailers, while organized crime might do it. In quadrant (3), recreational hackers may in theory attack public utilities but in practice these targets are more attractive to foreign services or cyberterrorists.

On these assumptions, it is possible to make predictions about companies' cybersecurity expenses. "The closer we are on the curve to the lower left corner, the higher the probability that the firm is investing a socially optimal amount in cyberdefense".[57] In this case, the expected social cost of an attack to a company in quadrant (4) is very low. If a retailer is knocked off by an attack, society has still other companies from which to buy services and products. Furthermore, given the unsophisticated characteristics of the attackers (these are not secret services), companies do not need to spend huge amount of money in cyberdefense. Therefore, the efficient level of cybersecurity expenditure for them is quite low. Retailers, financial institutions operate in competitive markets and the possibility for customers to switch to other suppliers give them right incentives to invest in cybersecurity, to avoid the loss of customers.

"The closer we are on y the curve to the upper right corner, the lower the probability that the firm is adequately investing in cybersecurity".[58] This is the opposite case of quadrant (4) and the expected social cost of a cyber-attack is enormous. The effects of an attack on a power grid will be vast not only for the utility's customers but also for the society as whole. Since the expected cost of such attacks will be massive, it is efficient to invest heavily in cybersecurity. The highly sophisticated attackers (foreign services, cyberterrorists) require an equally sophisticated cyberdefense. The socially optimal level of cybersecurity investment for these companies is very high. Furthermore, the monopolistic nature of the market in which these companies operate does not create the right incentives to invest in cybersecurity; since customers' exit is almost impossible, utilities have fewer incentives to offer a more secure service.

[57] Ibid, 11.
[58] Ibid..

The result of this analysis is that strategic companies (such us utilities) in less competitive market are less likely to adequately invest in cybersecurity than companies in competitive markets. Who should then be responsible for investing in cybersecurity so to secure these firms from the major cyber threats they face? Economics suggests that if the government is able to reduce the vulnerability more efficiently than a firm, it should pay; if the firm can do it more efficiently, it should pay for it. When it comes to major threats such as attacks from foreign services or cyberterrorism, the private sector is more able to identify cyber vulnerabilities, while the government has the comparative advantage at detecting sophisticated attacks, through, for instance, its own intelligence systems. It follows that, when the defense of the most sensitive systems is at stake, the responsibility for defending them should be shared through a **public-private partnership.**

What does this partnership look like? According to Nathan Sales: "All private firms might be asked to provide a baseline of cybersecurity – modestly effective (and modestly expensive) that are capable of thwarting intrusions by adversaries of low to medium sophistication. The government then should assume responsibility for defending public utilities and other sensitive enterprises against catastrophic attacks by foreign militaries and other highly sophisticated adversaries."[59]

The government, for instance, could provide companies with the intelligence on the type of attacks that it is likely to face. The NSA is already providing malware signature files to Google and some banks in order to help them to detect intrusions into their system.

3.3 Fight against cyberterrorism and international cooperation

The global reach of Internet and the related issues of jurisdiction and international organization become even more complex in the context of the development of organized cyberterrorism. Once it has been decided whether the government or the private sector or a private-public partnership should be developed to best fight cyber threats, there remains the question of whether local action is sufficient, i.e., whether domestic government is sufficient or international cooperation is necessary.[60]

There are ad hoc jurisdictional questions because the action in one country may have effects in another country. If the host country does not enforce the law against the cybercriminals, how can the victim country stop the attack? This uncertainty calls for international cooperation.

[59] Ibid, 12.
[60] See Trachtman , *Global Cyberterrorism*, 260-266.

In particular, Trachtman suggests four areas that require international cooperation: 1) limitations of terrorist access to networks; 2) *ex ante* surveillance, detection and interdiction of networks to repair the injury; 3) *ex post* identification and punishment of the attackers; 4) creation of more robust and resilient networks able to survive attacks. Furthermore, Trachtman proposes the creation of an umbrella organization, able to act transnationally and with jurisdiction over these matters.

3.4 Insuring against cyber risks

A complementary action that should be undertaken to minimize the financial losses is insuring against risk. However, it should be clear that this action should not substitute any initiative to avoid the security disaster. Insuring is not a preventive action but helps only in reducing the potential financial loss from the security breach. Furthermore, for the reasons previously explained, the market for security insurance is still in an early stage. It is quite complex to estimate the costs of security failures and only a clear definition of a taxonomy of major risks and available counter strategies can help in creating a more mature insurance market for cyber security.[61]

3.5 The role of National Cyber Security Strategies (NCSS)

Risk management of cybersecurity, Private Public Partnerships, international cooperation are the suggested approaches to best fight cybercrime and cyberterrorism. In this context, how are national governments worldwide implementing these solutions? It is worthwhile to look at the different national cybersecurity strategies that governments are implementing.

As society becomes more and more dependent on Information Technology, the protection and the availability of critical information assets are becoming a topic of national interest. Disruption of critical infrastructure and IT services could cause major negative effects on the overall economy. As such, securing cyberspace is becoming one of the most relevant challenges of the 21st century.

For this reason, many countries are considering cybersecurity as a strategic national issue and are designing and implementing National Cybersecurity Strategies. According to the European Network and Information Security Agency (ENISA), a national cyber security strategy "is a tool to improve the security and the resilience of national information infrastructures and services. It is a

[61] See Renda, *The puzzle in the bits*, 5.

high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such, it provides a strategic framework for a nation's approach to cyber security."

3.6 National Cybersecurity Strategies in Europe

The first national cybersecurity strategies started to appear in Europe in the first years of the previous decade.[62] In 2005 Germany adopted the *National Plan for Information Infrastructure Protection* (NPSI). In 2006 Sweden designed a *Strategy to Improve Internet Security in Sweden*. After the cyber attack in Estonia in 2007, this country was the first EU member state to adopt a comprehensive national security strategy in 2008. Since then, 10 EU Member states have designed a national cybersecurity strategy:

- **Estonia** (2008): It emphasizes the need for a secure cyberspace in general and it concentrates on information systems. The recommended initiatives are focused on regulation, education and cooperation.
- **Finland** (2008): Cyber security is primarily focused on the data security issue, on its economic importance for the development of the Finish information society.
- **Slovakia** (2008)**:** Information security is considered essential to the functioning and development of the society. Therefore, this country designs a comprehensive framework for cybersecurity focused on prevention, readiness and sustainability.
- **Czech Republic** (2011): key goals of this country's cybersecurity strategy are the protection against threats and mitigation of possible harms from attacks to the ICTs infrastructure.
- **France** (2011): The focus of this strategy is on fighting against cybercrime and establishing a cyber-defense for resisting events in cyberspace which could disrupt the availability, integrity or confidentiality of data.
- **Germany** (2011): Main focus is preventing and prosecuting cyber attacks, especially on critical infrastructures. It suggests also the provision of basic security functions certified by the state and the creation of an ad hoc task force to support the SMEs.
- **Lithuania** (2011): This country's cybersecurity strategy is focused on developing electronic information in an environment that protects confidentiality, integrity of personal data and privacy and safeguard information systems and critical information infrastructures against cyber-attacks.

[62] See ENISA (2012a).

- **Luxembourg** (2011): The strategy recognizes the importance of ICTs for citizens, society and economic growth and it is focused on the following items: Critical Information Infrastructure Protection, enhancing the regulatory environment, national and international cooperation, education and awareness and standards promotion.
- **Netherlands** (2011): The Netherlands tray to balance a safe and reliable ICTs, with no large scale disruptions with the need to enhance the freedom and openness of the Internet.
- **UK** (2011): The goal of this strategy is to make the UK the major economy of innovation, investment and quality in the ICTs field making the cyberspace safe for business and citizens by tackling the risks from cyberspace from criminals, terrorists and states.

However, according to ENISA, at the European and international level, a harmonized definition of cybersecurity is lacking and the understanding of key terms varies from country to country. For this reason, ENISA put forward a practical guide on development and execution of national cybersecurity strategies; it emphasizes the need of a cybersecurity strategy to improve the global resilience and security of national ICT infrastructures that enable critical functions of the state or the society. To design a cybersecurity strategy, ENISA advises to[63] take the following steps:

- Set the high level objectives to be accomplished in a given time frame by defining the vision and the scope of the strategy;
- Identify the business sectors and services relevant to this strategy;
- Undertake a comprehensive national risk assessment for choosing the objectives and scope of the strategy;
- Prioritize goals in terms of overall impact to the society and the economy;
- Take stock of the current enabling environment (policy, regulation, etc.),
- Achieve cooperation and agreement from the right stakeholders from the very beginning of the process;
- Define a road map for the implementation of the strategy according to the following steps:
    - Identify the specific activities that would meet the objectives of the strategy.
    - Design a governance framework for the implementation, evaluation and maintenance of the strategy.
    - Design a master plan for the implementation of the strategy.
    - Design specific action plans for each activity

[63] See Ibid. 8.

- Identify key performance indicators (KPIs) and ad hoc responsibilities to evaluate the strategy and its main actions.

3.7 European Union Cybersecurity Strategy

Furthermore, given the increase of economic espionage and state-sponsored activities in cyberspace, in February 2013, in a joint effort between the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, the European Union put forward its **Cybersecurity Strategy for an Open, Safe and Secure Cyberspace**[64] (hereafter EUCS) focused on five strategic priorities:

- Achieving cyber resilience;
- Drastically reducing cybercrime;
- Developing cyberdefence policy and capabilities related to the Common Security and Defense Policy (CSDP);
- Developing the industrial and technological resources for cybersecurity;
- Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

3.7.1 Achieving cyber resilience

To sustain cyber resilience in the EU, public and private sectors must develop capabilities and cooperate effectively. The European Commission has already developed a policy on Network and Information Security (NIS)[65] and it is negotiating with Council and Parliament a stronger and more modern mandate for ENISA. Furthermore it is considering legislation to:

- Define common minimum requirements for NIS at the national level that would include the set up of a well-functioning Computer Emergency Response Team (CERT), the design and implementation of a national NIS strategy and NIS cooperation plans. A "CERT-EU" responsible for the security of the IT system in the EU was create in 2012;
- Set up ad hoc mechanism to allow the coordination among the national NIS authorities;

[64] See European Union (2013)

[65] In 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298); in 2006, it adopted a Strategy for a Secure Information Society (COM(2006)251). Since 2009, the Commission has also adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; and COM(2011)163, endorsed by Council Conclusions 10299/11).

- Improve readiness and the engagement of the private sector in developing its own cyber resilience capabilities and share best practices across sectors. However, the Commission recognizes that private sectors still lack effective incentives to share reliable data on security breaches and cyber-attacks and to embrace a risk management culture or to invest in cyber security. For this reason, the Commission is proposing ad hoc legislation aiming at guaranteeing that players in key strategic sectors such as energy, transport banking assess and manage properly the cybersecurity risks that they face and share information on relevant security incidents with national NIS authorities. However, legal obligations should not substitute or prevent, voluntary and informal cooperation on security matters such as the European Public-Private Partnership for Resilience (EP3R);[66]
- Design and practice cyber incident exercises at EU level to enhance cooperation among the Member States and the private sector;
- Raise awareness among end users of the risks they face on line and of the simple steps they have to take to protect themselves. Ad hoc events such as the "European Cybersecurity Month" are initiative in this direction.

3.7.2 Drastically reducing cybercrime

The EUCS will focus on 3 items:

- **Strong and effective legislation.** There is a need in the EU for effective legislation against Cybercrime. The Commission will ensure the transposition and implementation of the cybercrime related directives and will encourage the Member states that have not yet ratified the **Council of Europe's Budapest Convention on Cybercrime** to ratify and implement it;
- **Enhanced operational capability to combat cybercrime.** Using its funding programs to allow Member States to identify security gaps. Through the Joint Research Center and the recently created European Cybercrime Center (EC3) within Europol and with Eurojust, identify best practices and best available techniques to identify cyber threats;
- **Improve coordination at the EU level.** The EU can enhance the Member States work by fostering a coordinated and collaborative approach by law enforcement and judicial authorities and public and private players from the EU and beyond.

[66] The European Public-Private Partnership for Resilience was launched via COM(2009)149

3.7.3 Developing cyberdefence policy and capability related to the framework of the Common Security and Defense Policy (CSDP)

Cyberdefense dimension is also very relevant for Cybersecurity in the EU and cyberdefense capabilities should be focused on detection, response and recovery from sophisticated cyber threats. Furthermore, the complex nature of this threats call for strong synergies between civilian and military approaches. The EUCS suggests to assess operational EU cyberdefense requirements and to promote EU cyberdefence capabilities through coordination between civilian and military actors in the EU, promoting dialogue with international partners, including NATO and other international organizations.

3.7.4 Developing industrial and technological resources for cybersecurity

The EUCS notices that it is very important to ensure that HW and SW security systems, developed in the EU and in third countries, are trustworthy, secure and able to protect personal data. Two are the main goals of the EUCS on this issue:

- **Promoting a Single Market for cybersecurity products.** To guarantee a high level of security, it is necessary that all players in the value chain (manufacturers, software developers, services providers) have the right incentive to achieve this goal and this should be true all over Europe. The development of a European wide market for highly secure products will help to achieve this goal. The European Commission will work in this direction through promoting in 2013 **a platform for NIS solutions** aimed at developing incentives for the adoption of secure ICT solutions in Europe. Furthermore, it will require major providers of hardware and software to communicate detected vulnerabilities to national authorities. The platform should stimulate the a**doption of industry-led security standards** and improve the information available to the public by developing security labels to help consumers in choosing their products.
- **Fostering R&D investments and Innovations.** Improving European R&D will foster a strong security market and reduce European dependence on foreign technologies. The European Commission will use Horizon 2020 to address the new critical area of research for ICT privacy and security. Furthermore, it invites Member States to use public procurement in order to stimulate the development and the adoption of better ICT security features and to improve **harmonized metrics for calculating risk premiums**, in cooperation with the insurance sector so to allow companies that have invested in security to access lower risk premiums.

3.7.5 Establishing a coherent international cyberspace policy for the European Union and promoting EU core values

The EU will promote openness and freedom of expression of the Internet as its main international cyberspace policy and will participate actively internationally in building cybersecurity capacity.

In order to address global challenges in cyberspace, the EU will cooperate with organization active in this field such as the Council of Europe, OECD, UN, OCSE, NATO, AU, ASEAN and OAS. At the bilateral level, it will cooperate with the United States especially in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

3.8 Cyber Security Strategies of non EU Countries[67]

3.8.1 United States of America

In 2003, the United States of America published the National Strategy to secure Cyberspace as part of the overall National Strategy for Homeland Security. Instead in May 2011, the USA released the International Strategy for Cyber Space based on a cooperative effort among government, international partner and private sector. The strategy is focused on:

- Promoting international security standards and open markets;
- Enhancing Networks security, reliability and resilience;
- Law enforcement based on enhancing collaboration and the rule of Law;
- Cyberdefence to be ready for the 21st Century Security Challenges;
- Fostering effective and inclusive structure for the governance of Internet;
- Building capacity for International development;
- Supporting Internet Freedom and privacy.

In February 2013, the White House issued an executive order conceived to improve the Cybersecurity of USA critical infrastructures (CI). Mentioning repeated intrusions into critical infrastructure and growing cyberthreats, the executive order 13636, *Improving Critical Infrastructure Cybersecurity*, aims at enhancing security and resilience through collaborative efforts involving federal agencies and private owners and infrastructures operators.

[67] See Ibid. 7, OECD (2012b) and CRS (2013).

3.8.2 Canada

Canada released *Cyber Security Strategy* in 2010; it focuses on four main activities:

- Guaranteeing security of government systems, through establishing clear roles and responsibilities, strengthening the security of Federal cyber systems and increasing awareness through the public administration;
- Securing vital cyber systems outside the Federal government through partnering initiatives with the provinces and the territories and with private and critical infrastructures sectors;
- Combating cybercrime and protecting Canadians citizens on line, with a special focus on protecting privacy;
- Promoting active international cooperation based on active, multilayered approach to international engagement on cyber security.

3.8.3 Japan

Japan released its *National Cybersecurity Strategy* in May 2010. It is focused on 5 pillars:

- Realize safety and security in the nation's life through developing policies able to neutralize possible outbreaks of cyber-attacks and to create response organizations;
- Implementation of policies that enhance national security and crisis management expertise in cyberspace;
- Developing of an information security policy focused on the nation's/users' viewpoint;
- Implementing a security policy that contributes to the growth of the overall economy;
- Building up international cooperation and alliances.

3.9 Cyber space global governance and response to cybercrime and cyberterrorism

The *National Cyber Security Strategies* presented earlier, envisage a common approach to fight cybercrime and cyberterrorism with the goal of: 1) establishing Computer Emergency Response Teams; 2) improving the coordination among the Security National Authorities; 3) enhancing the process of information sharing between the private sectors and the public authorities; 4) establishing private public partnerships to define best responses to cyber threats and improve trust between public and private players as suggested by the E3PR; 5) developing industrial and technological resources for cybersecurity such as industry lead security standards; 6) fostering

security R&D investments and Innovations; 7) designing in cooperation with the insurance sector, harmonized metrics for calculating risk premiums to allow for a more mature insurance market for cybersecurity.

However, the area that still requires better design and stronger commitment from the different players is the area of international coordination in the fight against cybercrime and cyberterrorism and its overall link to the cyber space global governance.

Given the increasing role today played by the Internet, it is not possible, even in democracies, to leave its use to users and service providers to govern. The cyber space is not any more a private space but a public area subject to the influence and the jurisdiction of individual states.

Therefore, a compromise is necessary to guarantee that the cyberspace is both free and secure, where freedom of expression, knowledge and business should be protected from the "Big Brother gaze of governmental, intergovernmental, commercial or criminal groups."[68]

Cyberspace should be viewed as a common domain, together with the land, the sea, the air and the space; consequently, as the other domains, it has a specific need for coordination and cooperation among all states.

As has been mentioned before, the fight against cyberterrorism requires a strong international cooperation. This calls for an international agreement and a coherent and global approach to deal with cybersecurity and cyber-attacks that should be based on a strong commitment between all players and relevant stakeholders at national and international levels. There is a need for an **International Treaty** that establishes a common understanding of what constitutes cybercrime, cyberwarfare and other forms of cyber threats. It is necessary to harmonize cybercrime legislations, making effective international justice and police cooperation. As suggested by Ghemaouti: "A global treaty at the level of the United Nations should establish the principle that serious crimes against peace and security perpetrated through the Internet and cyberspace are crimes under international law, whether they are punishable under national law. The most serious crimes in the cyberspace should be defined and handled under international law."[69]

The Council of Europe Convention on CyberCrime (2001) - ratified on July 2004 - was a first step in this direction. However, it has two basic limits: 1) it is still a regional initiative that is used as reference by many states, but lacking the necessary global framework;[70] 2) according to Trachtman,[71] the Cybercrime Convention is more oriented toward law enforcement after the

[68] See Ghernaouti, Cyber Power, 40.
[69] Ibid, 412.
[70] Ibid.
[71] Trachtman, *Global Cyberterrorism*, 268.

commission of crime rather than interdiction of crime or cyberterrorism. In other words, it is **a cybercrime law enforcement convention not a cyberterrorism convention.**

The creation of a global treaty on cybersecurity and cybercrime will require a leading role by the states and a strong collaboration from the private sector and the civil society. In this context, while it is important to recognize that currently, there is no credible alternative to the multi-stakeholder model for the governance of the cyberspace; it is important to stress that the United States should realize that key Internet assets cannot be controlled only by US companies, since it is important to share with other nations the networks oversight. Therefore, ICANN, as a global private Internet regulator, should become more transparent, more international and more accountable for its decisions.[72] A more balanced approach to the Cyberspace governance from the US and the Western world would also contribute to create more trust among countries as a necessary step to fight cybercrime and reduce geopolitical rivalry.

Overall, the adoption of a cyberspace treaty and the implementations of control measures to ensure that the treaty is respected will be a long process but it would contribute to connect the world in a more responsible way. Accordingly, it is important to move towards this direction now: the stakes are very high because Internet and the cyberspace are now part of our civilization.

[72] See on this Renda, "The Puzzle in the Bits," 5.

4. Conclusions

The title of this work "The Economics of Cyberterrorism: the Many Sides of the Prism", encompasses the complexity of such a phenomenon in the geometric form of the prism. The prism is a polyhedron (from Greek poly- meaning "many" and -edron meaning "face") i.e. a solid with many flat faces (cybercrime, cyberwarfare, cyberterrorism, etc.). Yet, the light through the prism leads the way towards an urgent need to enhance and strengthen international cooperation to mitigate cyberthreats, prevent cyberattacks, and enhance cybersecurity.

The Internet today has transformed our life connecting people, offering business opportunities and providing services to citizens. It is considered a critical infrastructure because it serves communications between communities, businesses, industrial and distribution entities, medical and emergency services, military operation as well as air and sea traffic control systems. It is so important to our western way of life that it is a viable target for those seeking to assert their influence and agendas on the rest of humanity. Therefore, the reliance on the Internet creates opportunities for cyber-attacks. Cybercrime-including fraud, identity theft and the creation and operation of botnets, is becoming more widespread and increasingly sophisticated. In the last years, there has been an escalating sequence of cyber-attacks involving, in some cases, millions of people across the Internet. The rate of growth and sophistication in cyber-attacks has affected national interests and required governments to adjust their national security and national defense strategies.

Furthermore, many reports have shone light on cyber-espionage practices conducted by state or state agents and there is a growing attention on the widespread use by terrorist groups of the web as a way to finance their activity, to recruit activists, to provide instructions on how to build and operate weapons and how to avoid detection by law enforcement computer technology. While many security experts agree that a cyber-attack would be most effective, if it were used to amplify a conventional bombing, they disagree about whether a widespread coordinated cyber-attack by terrorists is a near-term or long-term possibility. Terrorists may also be developing links with cybercriminals that will allow them to have access to high level computer skills.

This analysis pointed out that the physical forms of cyberterrorism, cyber warfare and cybercrime often look very much alike. The real difference lays in the intention of the attacker. In practice, the difference between cyber warfare and cyberterrorism is that cyberterrorism causes fear and damage to anyone in the vicinity, while cyber warfare has a defined target in a war (ideological or declared). Furthermore, quite often the term cybercrime is used by the law enforcement agencies to mean a crime committed through the use of information technology.

The scale of these cyber-attacks varies among users, consumers or business, depends on devices used but is becoming more and more pervasive due to the ability of the attackers to use the most common applications and the most used websites. It is striking to discover that a population greater than the European Union, 556 million citizens, is victimized every year by cybercrime: 1.5 million people per day, 18 victims per second! Furthermore, cybercrime is changing face, going mobile and going social! As 2 out of 3 adults use a mobile device to access the Internet, mobile vulnerabilities doubled in 2011 from 2010. At the same time, 4 out of 10 social network users have fallen victim to cybercrime on social networking platforms in 2011.

The size and the effects of these strikes are relevant. Quantifying their economic impact is quite a complex task due to the limited ability to measure the costs and probability of cyber-attacks. There are no standard methodologies for cost measurement and the analysis of the probability of cyber-attacks is hindered by the reluctant behavior of organizations to make publicly available their own information on security breaches. The costs of this disclosure can be significant- financial market impacts, reputation effects, litigation and liability concerns-, while the benefits of improved disclosure – more efficacy and cost savings in security- usually are slow to arrive and benefit all firms (including competitors). The unbalance between costs (sustained by a firm) and benefits (occurring to all) generates a market failure.

Several security consulting companies, such as Symantec, Cisco, Websense, run surveys and produce estimates of the costs and the losses due to cybercrime activities. The most recent estimates clustered by consumer and business sectors: they run from $1 trillion as overall impact, to $100,000 as average loss for an individual firm. Overall, the values vary significantly but are all quite relevant!

A more objective measure of the economic impact of these phenomena leads to study the effect at the micro and the macro level. The former effect is captured by looking at the effect of cyber-attacks on stock prices of individual firms. Some firms will be more exposed to cyber-attack than others and company's size will play a role. However, what will probably make a difference is the different level of dependence on computer networks in conducting their business that characterizes some firms compared to others. Traditional "brick and mortar" firms will be the least exposed to cyber-attack, compared to "click and mortar" that conduct their business both on and off line, or internet firms that conduct their business exclusively on line. Furthermore, the extent to which a firm is affected might reasonably be linked to the type of attack. Denial of service (DoS) attack causes a temporary interruption of the company's capabilities of running their business. Instead, security breaches are the ones that have the most lasting effects on the targeted firm,

because imply the theft or destruction of data. Overall, the literature shows that, other things being equal, the more the firm depends on the Internet and the more intrusive is the attack, the more likely the attack will generate significant financial impact on the firm.

The economic relevance of the impact of cyber-attacks is also confirmed by the way in which the insurance industry started to approach cyber-attack risks. As these risks became larger and more common with the diffusion of the Internet, the reaction of the insurance followed two paths. First, they made clear that existing business insurance did not include coverage of cyber-risks. Second, they started to introduce ad hoc policies to cover these type risks that were not included in previous coverage packages.

After looking at the economic impact of cyber-attacks at the firm level, the analysis focused on the repercussion of cyber-attack on the economy as whole. There is broad evidence that the Internet and communications infrastructure is considered today a key platform to conduct business, connect people and provide government services. Therefore, any Internet services block or denial is causing big economic losses. Using the OECD estimates of the economic impact of the shutdown of Internet and communications services during the Arab Spring in February 2011, service block and denial of Internet services have a significant impact on the overall economy.

As for the difference between the effects of cyberterrorism and other types of attacks, the review of the literature shows that its effects are more pervasive and can cause greater losses. According to many experts, cyberterrorists will try to combine physical attacks with cyber-attacks. Their action is very much focused on critical infrastructures: energy, transportation, telecommunications, water supply and waste management, agriculture and food supply, finance, public health, and essential government services. Furthermore, cyberterrorists are politically or religiously motivated. Generating terror among civilians and disrupting public and private infrastructure is their goal. Therefore, compared with common hackers, cyberterrorists are more dangerous. Common hackers prefer instant payoffs and act like shoplifters. They are opportunistic and cannot dedicate a long time to intruding into a single organization. The literature suggests that, because common hackers are likely to cause less damage a lower level of security investment can deter them. However, if an organization is attractive to cyberterrorists because of the information it holds or its role in critical infrastructure, the Information System Security level should be higher.

Given the variety of means and intensity of cybercrime described so far, what could be an optimal response to these threats and how can be properly designed? The analysis of literature suggests that:

1) First, security is never definitely achieved: the constant evolution of needs, systems threats and risks means that all security measures are potentially only temporary. The optimal level of cyber intrusions is not zero and the optimal level of cybersecurity expenditure is not infinity. Therefore, **cybersecurity needs to be considered as a form of risk management,** i.e. the willingness to master the risks linked to the use of information technologies and the costs generated by the protection of information systems from threats. Risk, vulnerability and threat are the key variables to be considered. Understanding the threats is one of the most critical issue of this process and also the one that has attracted the focus of the industry the most. As the number of threats discovered each year has sky rocked, the idea of being able to neutralize each threat has lost effectiveness. Therefore, the industry has been searching for a methodology to narrow down threats in a practical manner that allows efforts prioritization and optimal resources management. For instance, Intel Information Technology Security has developed the Treat agent risk assessment (TARA) that identifies the most likely attack vectors to support the development of optimal security strategies. TARA methodology identifies which threat agents pose the greatest risk, their motivation, methods and objectives and how they map to existing controls, not on the weak points themselves.

2) Second, once the risks have been assessed, the objective of information security and counter measures to fight cybercrime is not to make money but to avoid losing it, since the effect of a security accident generates either direct financial losses or indirect harm. Therefore, it is necessary to define the **efficient level of cybersecurity**. From an economic standpoint, the optimal result is not to prevent all attacks but to have an efficient level of attacks, in which, the investment in cyber security to prevent the attack should not be greater than the security gains. However, in this context, a critical question is: are individual firms and society as whole investing the right amount in cyberdefense? In particular, because the protection against cyberterrorism implies protection of critical infrastructures, mostly owned by the private sector, it is reasonable to ask: do private players have sufficient capabilities and incentives to invest appropriately in cybersecurity or is government intervention required? This work shows that the answer depends on the degree of competition of the market in which the attacked firm operates and the nature of the attacker (recreational hacker, foreign secret service or cyberterrorist). More exactly, strategic companies (such as utilities) in less competitive market are less likely to adequately invest in cybersecurity than companies in competitive markets. The question then becomes who should be responsible for investing in

cybersecurity? Economics suggests that if the government is able to reduce the vulnerability more efficiently than a firm, the government should pay; if the firm can do it more efficiently, then the firm should pay for it. When it comes to major threats such as attacks from foreign services or cyberterrorism, private sector is more able to identify cyber vulnerabilities, while the government has the comparative advantage at detecting sophisticated attacks, through, for instance, its own intelligence systems. It follows that, when the defense of the most sensitive systems is at stake, the responsibility for defending them should be shared through **a public-private partnership** in which all private firms might be asked to provide a baseline of cybersecurity – modestly effective (and modestly expensive) that are capable of thwarting intrusions by adversaries of low to medium sophistication. The government then should assume responsibility for defending public utilities and other sensitive enterprises against catastrophic attacks by foreign militaries and other highly sophisticated adversaries.

3) Third, once it has been decided whether the government or the private sector or a private-public partnership should be developed to fight at best cyber threats, there remains the question of whether local action is sufficient, i.e., whether domestic government is sufficient or **international cooperation is necessary**. The global reach of Internet and the related issues of jurisdiction and international organization become even more complex in the context of the development of organized cyberterrorism. There are ad hoc jurisdictional questions because the action in one country may have effects in another country. If the host country does not enforce the law against the cybercriminals, how the victim country can stop the attack? This uncertainty calls for international cooperation in four areas 1) limitations of terrorist access to networks, 2) ex ante surveillance, detection and interdiction of networks to repair the injury; 3) ex post identification and punishment of the attackers; 4) creation of more robust and resilient networks able to survive attacks. Furthermore, the creation of an umbrella organization, able to act transnationally and with jurisdiction over these matters, is proposed.

4) Finally, the present analysis discusses the **National Cyber Security Strategies** released in Europe and outside the EU in the past years. They envisage a common approach to fight cybercrime and cyberterrorism. An area that still requires better design and stronger commitment from the different players is that of international coordination and its link to the cyber space global governance. The analysis suggests viewing cyberspace as a common

domain, together with the land, the sea, the air and the space that, as the other domains, has a specific need for coordination and cooperation among all states. This calls for an international agreement and a coherent and global approach to deal with cybersecurity and cyber-attacks, based on a strong commitment between all players and relevant stakeholders at national and international levels. There is a need for an **International Treaty** that establishes a common understanding of what constitutes cybercrime, cyberwarfare and other forms of cyber threats. It is necessary to harmonize cybercrime legislations, making effective international justice and police cooperation. A global treaty at the level of the United Nations should establish the principle that serious crimes against peace and security perpetrated through the Internet and cyberspace are crimes under international law, whether they are punishable under national law. The most serious crimes in the cyberspace should be defined and handled under international law. The creation of a global treaty on cybersecurity and cybercrime will require a leading role by the states and a strong collaboration from the private sector and the civil society. In this context, while it is important to recognize that currently, there is no credible alternative to the multi-stakeholder model for the governance of the cyberspace, it is important to stress that the United States should realize that key Internet assets can't be controlled only by US companies, as it is important to share with other nations the networks oversight. A more balanced approach to the cyberspace governance from the US and the western world, would also contribute to create more trust among countries as a necessary step to fight cybercrime and reduce geopolitical rivalry. Overall, the adoption of a cyberspace treaty, and the implementations of control measure to ensure that the treaty is respected, will be a long process but it would contribute to connect the world in a more responsible way. For this reason, it is important to move towards this direction now: the stakes are very high because Internet and the cyberspace are now part of our civilization.

5. Bibliography

Abadie Alberto and Javier Gardeazabal, "The Economic Costs of Conflict," *The American Economic Review*, 93, 1, March 2003: 113-132, http://www.hks.harvard.edu/fs/aabadie/eccp.pdf

Anderson Ross, Moore Tyler, "The Economics of Information Security", 2006. *Science* 314(5799).

Bernam Eli, *Radical, Religious and Violent: The New Economics of Terrorism*, Cambridge, MA: MIT, 2009.

Cashell Brian, William D. Jackson, Mark Jickling, and Baird Webel, *The Economic Impact of Cyber-Attacks*, Congressional Research Service, April 1, 2004, https://www.fas.org/sgp/crs/misc/RL32331.pdf

Chen, Andrew H. and Thomas F. Siems, "The Effects of Terrorism on Global Capital Markets," *European Journal of Political Economy,* 20, 2004: 349–366.

CircleID (2013), "North Korea Suffers Internet Outage, U.S. Blamed," March 15 http://www.circleid.com/posts/north_korea_suffers_internet_outage_us_blamed/

Cisco, *Annual Security Report*, 2013, https://grs.cisco.com/grsx/cust/grsCustomerSurvey.html?SurveyCode=6653&KeyCode=000204094

Cronin Audry Kurt, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, Princeton: Princeton University Press, 2011.

CRS (2007), *Terrorist Capabilities for Cyber-attack: Overview and Policy Issues*, Congressional Research Service-The Library of Congress, Order Code RL33123

CRS (2013), *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress,* Congressional Research Service – The Library of Congress, R42894

Curran Kevin, Kevin Concannon and Sean McKeever, "Cyber Terrorism Attacks" in Janczewski Lech J. and Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism*, Hershey (PA): Information Science Reference, 2008: 1-6

Desouza Kevin C. and Tobin Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism," *Technological Forecasting and Social Change*, 70, 4, 2003: 385–396.

Dickey Christopher, R.M. Schneiderman, Babak Dehghanpisheh, "The Shadow War," *Newsweek*, December 13, 2010

Dyer Geoff, "Intelligence Chief in US Cyber-attack Warning," *Financial Times*, March 13, 2013.

Eldor Rafi and Rafi Menlick, "Financial Markets and Terrorism," Arison Business School, The Interdisciplinary Center, Herzliya, 2004, http://www.idc.ac.il/publications/files/111.pdf

Embar-Seddon, Ayn, "Cyberterrorism," *American Behavioral Scientist*, 45, 6, 2002: 1033–1043.

ENISA (2012a), *National Cybersecurity Strategies*: *Setting the course for national efforts to strengthen security in cyberspace.* May, Heraklion.

ENISA (2012b), *National Cybersecurity Strategies, Practical Guide on Development and Execution,* December, Heraklion.

European Commission (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels.

Foltz, Bryan C., "Cyberterrorism, Computer Crime, and Reality," *Information Management & Computer Security*, 12, 2/3, 2004: 154–166.

Gengler, B., "Politicians Speak Out on Cyberterrorism," *Network Security*, 10, 1999: 6.

Ghernaouti Salange, *Cyber Power, Crime, Conflict and Security in Cyberspace*, EPFL Press, 2013

Gordon, S., and Ford, R., "Cyberterrorism?" *Computer & Security*, 21, 7, 2002: 636–647.

Gordon Lawrence A. and Martin P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5, 4, 2002: 438–457.

Grady Mark F. and Francesco Parisi eds., *The Law and Economics of Cybersecurity,* Cambridge University Press, 2006.

Hua Jian and Bapna Sanjay, "The Economic Impact of Cyber Terrorism," *The Journal of Strategic Information System*, 22, 2, June 1, 2013: 175-186.

INTEL (2007), *Threat Agent Library Helps Identify Information Security Risks*, White Paper Intel Information Technology-

INTEL (2009), *Prioritizing Information Security Risks with Threat Agent Risk Assessment Agent*, White Paper Intel Information Technology.

ITU (2012) ,*ITR Final Acts*, http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

Janczewski Lech J. and Andrew M. Colarik, ed., *Cyber Warfare and Cyber Terrorism*, Hershey (PA): Information Science Reference, 2008.

Ksetri Nir, *Cybercrime and Cybersecurity in the Global South*, 2013, London: Palgrave Macmillan.

LECG, *Economic Impact of Broadband: An Empirical Study*, Final Report per Nokia Siemens Network, February 22, 2009, http://www.connectivityscorecard.org/images/uploads/media/Report_BroadbandStudy_LECG_March6.pdf

McAfee (2011), *In the Dark : Crucial Industries Confront Cyber-attacks*, CSIS

Mandiant, *M-Trends 2013*: *Attack the Security Gap*, 2013, https://www.mandiant.com/resources/m-trends/#

Manshaei Mohammad Hossein, Quanyan Zhu, Tansu Alpcan, Tamer Basar and Jean-Pierre Hubaux, *Game Theory Meets Network Security and Privacy, (2011),* ACM Computing Surveys.

Markoff John, "A Code for Chaos," *New York Times*, October 2, 2010, http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html

Moyar Mark, *A Question of Command: Counterinsurgency from the Civil War to Iraq*, New Haven, CT: Yale Library of Military History, 2009.

Mueller Milton, "ITU Phobia: Why WCIT Was Derailed," *Internet Governance Project* - IGP blog, 2012, http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/

Naím Moisés, "The Five Wars of Globalization," *Foreign Policy*, 134 (Jan. - Feb., 2003): 28-37.

Nakashima, Ellen, "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat," *Washington Post*, March 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html (retrieved 9/10/ 2013).

OECD (2003), *The Sources of Economic Growth in OECD Countries*, Paris: OECD Publishing, doi: 10.1787/9789264199460-en

OECD (2004), *The Economic Impact of ICT: Measurement, Evidence and Implications*, Paris: OECD Publishing, doi: 10.1787/9789264026780-en

OECD (2008), "Broadband and the Economy," OECD *Digital Economy Papers*, No. 146, Paris: OECD Publishing, doi: 10.1787/230450810820

OECD (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, Paris: OECD Publishing, 2009, doi: 10.1787/9789264056510-en

OECD (2011), "The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt", Paris: OECD http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html

OECD (2012a), *Internet Economy Outlook 2012*, Paris: OECD Publishing, 2012, doi: 10.1787/9789264086463-en

OECD (2012b), *Cybersecurity Policy Making at a Turning Point*, Paris, OECD http://www.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en

O'Neill Bard E., *Insurgency and Terrorism: From Revolution to Apocalypse*, Dulles, VA: Potomac Books, 2005.

Pape Robert, *Dying to Win: The Strategic Logic of Suicide Terrorism*, New York: Random House, 2005.

Petraeus David, *Counterinsurgency*, Department of the Navy. Headquarters. United States Marine Corps. Washington, DC, 15 December 2006: 4 http://www.fas.org/irp/doddir/army/fm3-24.pdf

Ponemon Institute, *Future State of IT Security: A Survey of IT Security Executives*, February 2012, http://www.ponemon.org/local/upload/file/Future_state_of_IT_Security_FINAL%207.pdf

Qiang Christine Z.W. and Carlo Maria Rossotto, *Economic Impacts of Broadband*, World Bank, Washington (DC), 2009.

Quocirca, "The Trouble Heading for Your Business," February 2013, http://www.quocirca.com/media/reports/022013/797/Quocirca%20-%20Targeted%20Attacks%20Feb%202013%20-%20final.pdf

Renda Andrea, *The puzzle in the bits: Cybersecurity, digital warfare and the future of Internet governance*, CEPS Commentary, 2013

Sales Nathan A., "Regulating Cybersecurity", forthcoming, *Northwestern University Law Review*, n. 107, 2013.

Schneider Friedrich, Tilman Brück, Daniel Meierrieks, "The Economics of Terrorism and Counter-Terrorism: A Survey ," *CESifo*, Working Paper no. 3012, 2010, http://www.cesifo-group.de/portal/page/portal/DocBase_Content/WP/WP-CESifo_Working_Papers/wp-cesifo-2010/wp-cesifo-2010-04/cesifo1_wp3012.pdf

Schmidt Eric and Jared Cohen, *The New Digital Age*, London: John Murray Publisher, 2013.

Stanton, J.J., "Terror in Cyberspace," *American Behavioral Scientist*, 45, 6, 2002: 1017–1032.

Sullivan Bob, "Is Flame Virus Fallout a Chinese, Russian Plot to Control the Internet?," 2012, http://redtape.msnbc.msn.com/_news/2012/06/12/12172042-is-flame-virus-fallout-a-chinese-russian-plot-to-control-the-internet?

Symantec, *Norton Cybercrime Report*, 2011, http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

Symantec, *Norton Cybercrime Report*, 2012, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Symantec, *Internet Security Threat Report*, 2012, 17, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

Symantec, *Internet Security Threat Report*, 2013, 18, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

The Economist (2010), "The Meaning of Stuxnet," September 30 http://www.economist.com/node/17147862

The Economist (2013), "A Giant Cage," April 6, http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled

Trachtman Joel P., "Global Cyberterrorism, Jurisdiction, and International Organization" in Grady Mark F. and Francesco Parisi eds., *The Law and Economics of Cybersecurity*, Cambridge University Press, 2006

Verizon, *Data Breach Investigation Report*, 2012, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf?r=43

Violino Bob, "Unseen, All-out Cyber War on the U.S. Has Begun," *InfoWorld*, January 28, 20l3, http://www.infoworld.com/d/security/unseen-all-out-cyber-war-the-us-has-begun-211438

Websense, *Threat Report*, 2013, http://www.websense.com/content/websense-2013-threat-report.aspx

Wehde, Ed, "US Vulnerable to Cyberterrorism," *Computer Fraud & Security*, 1, 1998: 6–7.