27

Cyber-Security

Myriam Dunn Cavelty

Chapter Contents

Reader's Guide

This chapter looks at why cyber-security is considered one of the key national security issues of our times. The first section provides technical background information. The second section unravels three different, but interrelated ways to look at cyber-security. The first discourse has a technical focus and is about viruses and worms; the second looks at the interrelationship between the phenomenon of cyber-crime and cyber-espionage; the third turns to a military and civil defence-driven discourse about the double-edged sword of fighting wars in the information domain and the need for critical infrastructure protection. Based on this, the third section looks at selected protection concepts from each of the three discourses. The final section sets the threat into perspective: despite heightened media attention and a general feeling of impending cyber-doom, the level of cyber-risk is generally overstated.

Introduction

Information has been considered a significant aspect of **power**, diplomacy, and armed conflict for a very long time. Since the 1990s, however, information's role in International Relations and security has diversified and its importance for political matters has increased, mostly due to the proliferation of **information and communication technology** (ICT) into all aspects of life in post-industrialized societies. The ability to master the generation, management, use but also manipulation of information has become a desired power resource since the control over knowledge, beliefs, and ideas is increasingly regarded as a complement to control over tangible resources such as military forces, raw materials, and economic productive capability. Consequently, matters of cyber-(in)-security—although not always under this name—have become a security issue.

In this chapter, the cyber-(in)-security logic is unpacked in four sections as described in the Reader's Guide, with the first providing the necessary technical background information on why the information infrastructure is inherently insecure, how computer vulnerabilities are conceptualized, who can exploit them, and in what ways.

Information security

Cyberspace connotes the fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange. A 'network ecosystem' is created; it is virtual and it 'exists everywhere there are telephone wires, coaxial cables, fibre-optic lines or electromagnetic waves' (Dyson et al. 1996). Cyberspace, however, is not only virtual, since it is also made up of servers, cables, computers, satellites, etc. In popular usage, the terms cyberspace and **Internet** are used almost interchangeably, even though the Internet is just one part of cyberspace.

Cyber-security is both about the insecurity created by and through this new place/space and about the practices or processes to make it (more) secure. In security policy, cyberspace has a double role: it serves both as an attack vector through which objects and services of value for the state and society can be threatened (in peace time and during conflict) and as a sphere of operations in which strategies and countermeasures against security threats are implemented and conducted. This way, cyber-security is not just about the security *of* cyberspace, but is also security created *through* cyberspace (Betz and Stevens 2011).

The inherent insecurity of computer networks

Today's version of the Internet is a dynamic evolution of the Advanced Research Projects Agency Network (ARPANET), which was mainly designed for optimized information exchange between the universities and research laboratories involved in United States Department of Defense (DoD) research. At the time, there was no apparent need for a specific focus on security, because information systems were being hosted on large proprietary machines that were connected to very few other computers. Therefore, the network designers emphasized robustness and survivability over security.

Due to the dynamic evolution of ARPANET, this turned into a legacy problem. What makes systems so vulnerable today is the confluence of the same basic network technology, the shift to smaller and far more open systems, both not built with security in mind, and the rise of extensive networking. In addition, the commercialization of the Internet in the 1990s led to an even bigger security deficit. There are significant market-driven obstacles to IT-security: there is no direct return on investment; time-to-market impedes extensive security measures; and security mechanisms have a negative impact on usability so that security is often sacrificed for functionality (Anderson and Moore 2006).

There are additional forces keeping cyberspace insecure: **Big Data** is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing strategies through personalized advertising and prediction of future consumer behaviour. Therefore, there is little interest in encrypted (and therefore secure) information exchange. On top of this, the intelligence agencies of this world have the same interest in data that can be easily grabbed and analysed. Furthermore, the **NSA revelations of 2013** have exposed that intelligence services are making cyberspace more insecure directly. In order to be able to have more access to data, and in order to prepare for future cyber-conflict, they buy and exploit so-called **zero-day**

vulnerabilities in current operating systems and hardware to inject malware into numerous strategically opportune points of the Internet infrastructure (Dunn Cavelty 2014).

Computer vulnerabilities and threat agents

The terminology in information security is often seemingly congruent with the terminology in national security discourses: it is about threats, agents, vulnerabilities, etc. However, the terms have very specific meanings so that seemingly clear analogies must be used with care. The focus of the cyber-security discourse are information *attacks* (both passive and active), defined as (potentially) damaging events orchestrated by a human adversary ('threat agents'). The most common label bestowed upon them is **hacker** (Erickson 2003). For members of the computing community, 'hacker' describes a member of a distinct social group (or sub-culture); a particularly skilled programmer or technical expert who knows a programming interface well enough to write novel software. A particular ethic is ascribed to this subculture: a belief in sharing, openness, and free access to computers and information; decentralization of government; and in improvement of the quality of life (Levy 1984). In popular usage and in the media, however, the term hacker generally describes criminals. In the cyber-security debate, hacking is seen as a modus operandi that can be used not only by technologically skilled individuals for minor misdemeanours, but also by organized actor groups with truly bad intent, such as terrorists or foreign states.

Hacking tools

The term for the tools used in a cyber-attack is **malware** (malicious + software). Well-known examples are *viruses and worms*, computer programs that replicate functional copies of themselves with varying effects ranging from mere annoyance and inconvenience to compromise of the confidentiality or integrity of information. There also are *Trojan horses*, programs that masquerade as benign applications but set up a back door so that the hacker can return later and enter the system. Often system intrusion is the main goal of more advanced attacks: if the intruder gains full system control, or 'root' access, he has unrestricted access to the inner workings of the system (Anonymous 2003). Very often, so-called *social engineering* techniques are used, whereby a human target is tricked into disclosing confidential information that helps the hacker to gain access to the system. Due to the characteristics of digitally stored information an intruder can delay, disrupt, corrupt, exploit, destroy, steal, and modify information. Depending on the value of the information or the importance of the application for which this information is required, such actions will have different impacts with varying degrees of gravity.

KEY POINTS

- Cyberspace has both virtual and physical elements. We tend to use the terms cyberspace and Internet interchangeably, even though cyberspace encompasses far more than just the Internet.
- Cyber-security is both about the insecurity created through cyberspace and about the technical and non-technical practices of making it (more) secure.
- The Internet started as ARPANET in the 1960s and was never built with security in mind. This legacy, combined with the rapid growth of the network, its commercialization, and several economic and strategic interests make computer networks inherently insecure.
- Information security uses a vocabulary very similar to national security language, but has specific meanings. Cyber-attacks are the main focus of the cyber-security discourse. Attackers are called hackers.
- The umbrella term for all hacker tools is malware. The main goal of advanced attacks is full system control, which allows the intruder to delay, disrupt, corrupt, exploit, destroy, steal, or modify information.

Three interlocking cyber-security discourses

The cyber-security discourse originated in the USA in the 1970s, built momentum in the late 1980s and spread to other countries in the late 1990s. The US government shaped both the threat perception and the envisaged countermeasures with only little variation in other countries. On the one hand, the debate was decisively influenced by the larger post-Cold War strategic context in which the notion of asymmetric vulnerabilities, epitomized by the multiplication of malicious actors (both state and non-state) and their increasing capabilities to do harm started to play a key role. On the other hand, discussions about cyber-security always were and still are influenced by the ongoing **information revolution**, which the USA is shaping both technologically and intellectually by discussing its implications for International Relations and security and acting on these assumptions.

The cyber-security discourse was never static because the technical aspects of the information infrastructure are constantly evolving. Most importantly, changes in the technical sub-structure changed the referent object. In the 1970s and 1980s, cyber-security was about those parts of the private sector that were becoming digitalized and about government networks and the classified information residing in it. The growth and spread of computer networks into more and more aspects of life changed this limited referent object in crucial ways. In the mid-1990s, it became clear that key sectors of modern society, including those vital to national security and to the essential functioning of (post-)industrialized economies, had come to rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. The referent object that emerged was the totality of **critical (information) infrastructures** that provide the way of life that characterizes our societies. Hacking incidents during the US elections in 2016—allegedly conducted by Russian nationals—have recently focused the debate on the issue of strategic manipulation—also called information warfare—and on the threat to democratic processes (Inkster 2016).

When telling the cyber-security-story we can distinguish between three different, but often closely interrelated and reinforcing discourses, with specific threat imaginaries and security practices, referent objects, and key actors. The first is a technical discourse concerned with malware (viruses, worms, etc.) and system intrusions. The second is concerned with the phenomena of cyber-crime and cyber-espionage. The third is a discourse driven initially by the US military, focusing on matters of **cyber-war** and **critical infrastructure protection** (see Figure 27.1).

	Technical	Crime–Espionage	Military/civil defence
Main actors	▪ Computer experts ▪ Anti-virus industry	▪ Law enforcement ▪ Intelligence community	▪ National security experts ▪ Military ▪ Civil defence establishment
Main referent object	▪ Computers ▪ Computer networks	▪ Business networks ▪ Classified information (government networks)	▪ Military networks, networked armed forces ▪ Critical (information) infrastructures

Figure 27.1 Three discourses

Table 27.1 Prominent malware

Name of malware	Year of discovery	Creator	Infected	Effect
Morris Worm	1988	Robert Morris (computer student), USA	UNIX systems	Slowed down machines in the ARPANET until they became unusable; huge impact on the general awareness of insecurity
Michelangelo	1992	(unknown)	DOS systems	Overwrote the first hundred sectors of the hard disk with nulls; caused first digital mass hysteria
Back Orifice	1998	Cult of the Dead Cow (hacker collective), USA	Windows 98	Tool for remote system administration (Trojan horse)
Melissa	1999	David L. Smith (programmer), USA	Microsoft Word, Outlook	Shut down Internet mail; clogged systems with infected e-mails
I Love You	2000	Two computer students, the Philippines	Windows	Overwrote files with copy of itself; sent itself to the first fifty people in the Windows Address Book
Code Red	2001	(unknown)	Microsoft web servers	Defaced websites; used machines for DDoS-attacks
Nimda	2001	(unknown)	Windows workstations and servers	Allowed external control over infected computers
Blaster	2003	18-year-old student, USA	Windows XP and 2000	DDos-attacks against 'windowsupdate.com'; side effects: system crash; was suspected to have caused black-out in USA (unconfirmed)
Slammer	2003	(unknown)	Windows 95–XP	DDoS-attacks; slowed down Internet traffic worldwide
Zeus	2007	(unknown), available in underground computer forums	Windows	Stole banking and other information; formed botnets
Conficker (several versions)	2008	(unknown)	Windows	Formed botnets
Stuxnet	2010	Attributed to US and Israeli government (Operation Olympic Games)	SCADA system (Siemens industrial software and equipment)	Spied on and subverted industrial systems
Duqu	2011	(unknown)	Windows	Looked for information useful in attacking industrial control systems; code almost identical to Stuxnet (copy-cat software)
Flame	2012	Attributed to US and Israeli government (Operation Olympic Games)	Windows	Cyber-espionage (mainly in the Middle East)
Regin	2014	Unknown, probably NSA; also used by British intelligence agency GCHQ	Windows	Targeted data collection
WannaCry	2017	(unknown)	Windows	Encrypted data and demanded ransom payments in Bitcoins

Viruses, worms, and other bugs (technical discourse)

The technical discourse is focused on computer and network disruptions caused by different types of malware. As early as 1988, the ARPANET had its first major network incident: the 'Morris Worm'. The worm used so many system resources that the attacked computers could no longer function and large parts of the early Internet went down. The devastating effects led to the setup of a centre to coordinate communication among computer experts during IT emergencies: a Computer Emergency Response Team (CERT). This centre, now called the CERT Coordination Center, still plays a considerable role in computer security today and served as a role model for many similar centres all over the world. Around the same time, the anti-virus industry emerged and with it techniques and programs for virus recognition, destruction, and prevention.

The worm also had a substantial psychological impact by making people aware just how insecure and unreliable the Internet was. While it had been acceptable in the 1960s that pioneering computer professionals were hacking and investigating computer systems, the situation had changed by the 1980s. Society had become dependent on computing in general for business practices and other basic functions. Tampering with computers suddenly meant potentially endangering people's careers and property; and some even said their lives (Spafford 1989). Ever since, malware as 'visible' proof of the persuasive insecurity of the information infrastructure has remained in the limelight of the cyber-security discourse; and it also provides the back-story for the other two discourses. Table 27.1 lists some prominent examples.

Most obviously, the history of malware is a mirror of technological development: the type of malware, the type of targets, and the **attack vectors** all changed with the technology and the existing technical countermeasures (and continue to do so). This development goes in sync with the development of the cyber-crime market, which is driven by the considerable amounts of money available to criminal enterprises at relatively low risk of prosecution. While there was a tongue-in-cheek quality to many of the early malware incidents, computer security professionals nowadays are increasingly concerned with the rising level of professionalization coupled with the criminal and strategic intent behind attacks. Advanced malware is targeted: a hacker picks a victim, scopes the defences, and then designs an operation and specific malware to get around them (Symantec 2010). The most prominent example for this kind of malware is Stuxnet (see Case Study 27.3). However, some IT security companies warn against overemphasizing so called **advanced persistent threat** attacks just because we hear more about them (Verizon 2010: 16). Only a very small percentage of all incidents are so sophisticated that they were impossible to stop. The vast majority of attackers go after small-to-medium-sized enterprises with bad defences.

KEY POINTS

- In 1988, the Morris Worm downed large parts of the early Internet, proving the theory right and making clear that the Internet was a very insecure technology.
- As a consequence, the CERT Coordination Center was founded. It is still very active today and has served as a model for similar computer emergency response teams in many countries.
- There is a long list of prominent malware, which often made headlines. Over the years, malware has become more sophisticated and more clearly linked to criminal and strategic intent.
- The most dangerous malware is tailored to a specific target for high effect. However, the large majority of attacks remain unsophisticated and go after small or medium-sized enterprises with little IT security awareness and/or investment.

Cyber-crooks and digital spies (crime-espionage discourse)

The cyber-crime discourse and the technical discourse are very closely related. The development of cyber-law in different countries plays a crucial role in the second discourse because it allows the definition and prosecution of misdemeanour. Not surprisingly, the development of legal tools to prosecute unauthorized entry into computer systems coincided with the first serious network incidents described here (cf. Mungo and Clough 1993).

Cyber-crime has come to refer to any crime that involves computers, like a release of malware or spam, fraud, and many other things. Until today, notions of computer-related economic crimes determined the discussion about computer misuse. However, a distinct national security dimension was established when computer intrusions (a criminal act) were linked to the more traditional and well-established espionage

Table 27.2 Cyber-crime and cyber-espionage

Name of incident	Year of occur-rence/discovery	Description	Perpetrators
414s break-ins	1982	Break-ins into high-profile computer systems in the USA	Six teenage hackers from Mil-waukee
Hanover Hackers (Cuckoo's Egg)	1986–8	Break-ins into high-profile computer systems in the USA	German hacker recruited by the KGB
Rome Lab incident	1994	Break-ins into high-profile computer systems in the USA	British teenage hackers
Citibank incident	1994	$10 million siphoned from Citibank and transferred the money to bank accounts around the world	Russian hacker(s)
Solar Sunrise	1998	Series of attacks on DoD computer networks	Two teenage hackers from California plus one Israeli
Moonlight Maze	1998	Pattern of probing of high-profile computer systems	Attributed to Russia
Titan Rain	2003–	Access to high-profile computer systems in the USA	Attributed to China
Zeus Botnet	2007	Trojan horse 'Zeus'; controlled millions of machines in 196 countries	International cyber-crime net-work; over 90 people arrested in US alone
GhostNet	2009	Cyber-spying operation; infiltration of high-value political, economic, and media locations in 103 countries	Attributed to China
Operation Aurora	2009	Attacks against Google and other companies to gain access to and potentially modify source code repositories at these high tech, security, and defence contractor companies	Attributed to China
Wikileaks Cablegate	2010	251,287 leaked confidential diplomatic cables from 274 US embassies around the world	WikiLeaks, not-for-profit activist organization
Operations Payback and Avenge Assange	2010	Coordinated, decentralized attacks on opponents of Internet piracy and companies with perceived anti-WikiLeaks behaviour	Anonymous, hacker collective
Theft of CO_2-Emission Papers	2011	Theft of 475,000 carbon dioxide emissions allowances worth €6.9 million, or $9.3 million	Attributed to or-ganized cyber-crime (purpose probably money laundering)
NSA revelations	2013	Leaking of classified information that showed the extent of (US government) surveillance programs through cyber-means	United States Na-tional Security Agency (NSA)
Sony Pictures Hack	2014	Series of hacks and data release about Sony international, cumulating in cancellation of movie *The Interview* (which shows violent death of North Korean leader Kim Jong Un)	Attributed to North Korea
Office of Personnel Management Data Breach	2015	Sensitive data about people who worked or applied for the US government stolen	Chinese govern-ment hackers (one arrested in August 2017)
US Election Hack	2016	Sensitive data about Democratic candidate stolen and leaked to influence public opinion (and to undermine faith in democratic process)	Attributed to Russian hacker collective

discourse. Early on, prominent hacking incidents—such as the intrusions into high-level computers perpetrated by the Milwaukee-based '414s'—led to a feeling in policy circles that there was a need for action (Ross 1991). If teenagers were able to penetrate computer networks that easily, it seemed only logical that better organized entities such as states would be even better equipped to do so. Indeed, events like the Cuckoo's Egg incident, the Rome Lab incident, Solar Sunrise, or Moonlight Maze made apparent that the threat was not just one of criminals or juveniles, but that foreign nationals could acquire classified or sensitive information relatively easily (see Table 27.2).

The so-called **attribution problem**—which refers to the difficulty in clearly determining those initially responsible for a cyber-attack plus identifying their motivating factors—is a big challenge in the cyber-domain. Due to the architecture of cyberspace, online identities can be optimally hidden. Blame on the basis of the 'cui bono'-logic (which translates into 'to whose benefit?') is not sufficient proof for legal prosecution, although it is often used in the political discourse. The challenges of clearly identifying perpetrators gives state actors convenient 'plausible deniability and the ability to officially distance themselves from attacks' (Deibert and Rohozinski 2009: 12).

There are three trends worth mentioning. First, tech-savvy individuals (often juveniles) with the goal of mischief or personal enrichment shaped the early history of cyber-crime. Today, professionals dominate the field. The Internet is a near-ideal playground for semi- and organized crime in activities such as theft (like looting online banks, intellectual property, or identities) or for fraud, forgery, extortion, and **money laundering**. Actors in the 'cyber-crime black market' are highly organized regarding strategic and operational vision, logistics, and deployment. Like many real companies, they operate across the globe.

Second, the **cyber-espionage** story has changed. For many years, it was mainly China that was made responsible for high-level penetrations of government and business computer systems in Europe, North America, and Asia. However, the NSA revelations in 2013 by Edward Snowden made clear that Western governments conduct massive data collection through cyberspace for strategic information gathering too, which has given the cyber-espionage discourse a new direction.

The third trend is the increased attention that **hacktivism**—the combination of hacking and activism—has gained in recent years. WikiLeaks, for example, has addedyetanothertwisttothediscourse.Actingunderthe hacker-maxim 'all information should be free', this type of activism deliberately challenges the self-proclaimed power of states to keep information, which they think could endanger or damage national security, secret. It emerges as a cyber-security issue because of the way the data was stolen (in digital form) but also how it was made available to the whole world through multiple mirror sites. Somewhat related are the multifaceted activities of hacker collectives such as Anonymous or LulzSec. They creatively play with anonymity in a time obsessed with control and surveillance and humiliate high-visibility targets by **DDoS-attacks**, break-ins, and the release of sensitive information. Furthermore, it seems more and more governments are accepting, if not sponsoring, hacktivist activities. Some of the most notorious cyber-incidents in the last years were allegedly conducted by hacker collectives with ties to the Russian government (See Case Study 27.1).

CASE STUDY 27.1 US election hack

Since 2015, several US institutions and the US Democratic National Committee (DNC) have been the victims of network intrusions. The perpetrators, said to be the Russian hacker groups 'APT28' and 'APT29', used spear-phishing emails to deliver Remote Administration Tools (RAT) malware. This way, the hackers were able to gain access to sensitive data. It was later published at strategic times during the US presidential elections, interfering in the democratic process and potentially helping the Republican candidate, Donald Trump, win the elections. In October 2016, the US government officially accused the Russian government of having ordered the network intrusions. A loss of trust in the legitimacy and integrity of the democratic process marked the incident.

More generally, the combination of hacking techniques combined with a strategic disinformation campaign started a new debate in the cyber-security discourse. That political actors attempt to manipulate public opinion is not new. What has changed, however, is the media environment: Web-based services and content and social media with its filtering algorithms open up new opportunities for 'media hacking'. Targeted manipulation of Internet-based content is a tactic that Moscow has been using for years. Since the Ukraine conflict it is known that Russia uses a 'troll army'—also called Kremlbots—to influence opinion in national and, increasingly, international web spaces through coordinated operations. A newer dimension is the intrusion into computer systems to discredit or blackmail political opponents. The combination of data theft and interference is, however, in line with the Russian idea of 'information warfare'. In contrast to the Euro-Atlantic view, which defines cyber-war narrowly as destructive attacks, Russia approaches the issue in a more holistic way: besides information systems, opinions have always been an important target of its information wars.

KEY POINTS

- The notion of computer crime and the development of cyber law coincided with the first network attacks. Although this discourse is mainly driven by economic considerations until today, political cyber-espionage, as a specific type of criminal computer activity started worrying officials around the same time.
- Over the years, cyber-criminals have become well-organized professionals, operating in a consolidated cyber-crime black market.
- As it is very hard to identify perpetrators who want to stay hidden in cyberspace (attribution problem), states can plausibly deny being involved.
- Politically motivated break-ins by hacker collectives that go after high-level targets, with the aim of stealing and publishing sensitive information or just ridiculing them by targeting their websites, add to the feeling of insecurity in government circles.

Cyber(ed) conflicts and vital system security (military–civil defence discourse)

The Gulf War of 1991 created a watershed in US military thinking about cyber-war. Military strategists saw the conflict as the first of a new generation of **information age** conflicts in which physical force alone was not sufficient, but was complemented by the ability to win the information war and to secure 'information dominance'. As a result, American military thinkers began to publish on the topic and developed doctrines that emphasized the ability to degrade or even paralyse an opponent's communications systems (cf. Campen 1992; Arquilla and Ronfeldt 1993).

In the mid-1990s, the advantages of the use and dissemination of ICT that had fuelled the revolution in military affairs were no longer seen only as a great opportunity providing the country with an 'information edge' (Nye and Owens 1996), but were also perceived as constituting an over-proportional vulnerability vis-à-vis malicious actors. Global information networks seemed to make it much easier to attack the US asymmetrically and, as such, an attack no longer required big, specialized weapons systems or an army: borders, already porous in many ways in the real world, were non-existent in cyberspace. There was widespread fear that those likely to fail against the American military would instead plan to bring the USA to its knees by striking vital points fundamental to the national security and the essential functioning of industrialized societies at home.

The development of military doctrine involving the information domain continued. For a while, **information warfare** remained essentially limited to military measures in times of crisis or war. This began to change around the mid-1990s, when these actions became operations targeting the entire information infrastructure of an adversary—political, economic, and military, throughout the continuum of operations from peace to war. NATO's 1999 intervention against Yugoslavia marked the first sustained use of the full spectrum of information operation components in combat. Much of this involved the use of disinformation via the media, but there were also website defacements, a number of DDoS-attacks, and rumours that Slobodan Miloševićs' bank accounts had been hacked by the US armed forces.

The increasing use of the Internet during the conflict gave it the distinction of being the 'first war fought in cyberspace' or the 'first war on the Internet'. Thereafter, the term cyber-war came to be widely used to refer to any phenomenon involving a deliberate disruptive or destructive use of computers. For example, the cyber-confrontations between Chinese and US hackers in 2001 were labelled the 'first Cyber World War'. The cause was a US reconnaissance and surveillance plane that was forced to land on Chinese territory after a collision with a Chinese jet fighter. In 2007, DDoS-attacks on Estonian websites were readily attributed to the Russian government, and various government officials claimed that this was the first known case of one state targeting another using cyber-warfare (see Case Study 27.2). Similar claims were made in the confrontation between Russia and Georgia of 2008. In other cases, China is said to be the culprit (see previous section and Table 27.3).

The discovery of Stuxnet in 2010 changed the overall tone and intensity of the debate (see Case Study 27.3).

Due to the attribution problem, it was impossible to know for certain who was behind this piece of code, though many suspected one or several state actors (Farwell and Rohozinski 2011). In June 2012, an investigative journalist suggested that Stuxnet is part of a US and Israeli intelligence operation and that it was programmed and released to sabotage the

CASE STUDY 27.2 Estonian 'cyber-war'

When the Estonian authorities removed a bronze statue of a Second World War-era Soviet soldier from a park, a cyberspace-'battle' ensued lasting over three weeks, in which a wave of so-called Distributed Denial of Service attacks (DDoS) swamped various websites—among them the websites of the Estonian parliament, banks, ministries, newspapers, and broadcasters—disabling them by overcrowding the bandwidths for the servers running the sites.

Various officials readily and publicly blamed the Russian government. Also, even though the attacks bore no serious consequences for Estonia other than (minor) economic losses, some officials even openly toyed with the idea of a counter-attack in the spirit of Article 5 of the North Atlantic Treaty, which states that 'an armed attack' against one or more NATO countries 'shall be considered an attack against them all'. The Estonian case is one of the cases often referred to in government circles to prove that there is a rising level of urgency and need for action.

Table 27.3 Instances of cyber(ed)-conflict

Name of incident	Year of occurrence	Description	Actors/perpetrators
Gulf War	1991	First of a new generation of conflicts that highlighted the importance of the information sphere in conflict	US military
Operation 'Allied Force'	1999	'The first Internet War'; sustained use of the full-spectrum of information warfare components in combat; numerous hacktivism incidents	US military, hacktivists from many countries
'Cyber-Intifada'	2000–5	E-mail flooding and Denial-of-Service (DoS) attacks against government and partisan websites during second Intifada	Palestinian and Israeli hacktivists
'Cyber World-War I'	2001	Defacement of Chinese and US websites and waves of DDoS-attacks after US reconnaissance and surveillance plane was forced to land on Chinese territory	Hacktivists from many nations (Saudi Arabia, Pakistan, India, Brazil, Argentina, Malaysia, Korea, Indonesia, Japan)
Estonia DDoS-attacks	2007	DDoS-attacks against websites of the Estonian parliament, banks, ministries, newspapers, and broadcasters	Attributed to Russian government
Georgia DDoS-attacks	2008	DDoS-attacks against numerous Georgian websites	Attributed to Russian government
Stuxnet	2010	Computer worm that might have been deliberately released to slow down Iranian nuclear programme	US government (+ Israel)
Korean network intrusions	2011	Botnets and DDos-attacks against government websites; experts suspected North Korean 'cyber-weapons' test	Attributed to North Korean government
Syrian Conflict	2011–	Frequent use of cyber-tools by many different actors for political means	Many different hacker groups
Ukraine Conflict	2013–	Russia's 'Test Lab' for cyber-war, targets of cyber-attacks: power grid, financial system and other infrastructures	Russian hacker groups

CASE STUDY 27.3 Stuxnet

Stuxnet is a computer worm that was discovered in June 2010 and has been called '[O]ne of the great technical blockbusters in malware history' (Gross 2011). It is a complex program. It is likely that writing it took a substantial amount of time, advanced-level programming skills, and insider knowledge of industrial processes. Stuxnet was the most expensive malware ever found at that time. In addition, it behaved differently from malware used for criminal intent: it did not steal information and it did not herd infected computers into so-called **botnets** from which to launch further attacks. Rather, it looked for a very specific target: Stuxnet was written to attack Siemens' *Supervisory Control And Data Acquisition* (SCADA) systems that are used to control and monitor industrial processes. In August 2010, the security company Symantec noted that 60 per cent of the infected computers worldwide were in Iran. It was also reported that Stuxnet damaged centrifuges in the Iran nuclear programme. This evidence led several experts to the conclusion that one or several nation states—most often named are the USA and/or Israel–were behind the attack. No official statement has ever been issued, but the involvement of the US government seems quite certain by now.

On another note, Stuxnet provided a platform for an ever-growing host of cyber-war experts to speculate about the future of cyber-aggression. Internationally, Stuxnet has had two main effects: first, governments all over the world are currently releasing or updating cyber-security strategies and are setting up new organizational units for cyber-defence (and -offence). Second, Stuxnet can be considered a 'wake-up' call: ever since its discovery, increasingly serious attempts to come to some type of agreement on the non-aggressive use of cyberspace between states have been undertaken.

Iranian nuclear programme. For many observers, Stuxnet as a 'digital first strike' marks the beginning of the unchecked use of **cyber-weapons** in military-like aggressions (Gross 2011). However, other reports think this unlikely (cf. Sommer and Brown 2011), mainly due to the uncertain results a cyber-war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks.

Future conflicts between nations will most certainly have a cyberspace component but they will be just a part of the battle. It is therefore more sensible to speak about cyber(ed) conflicts, conflicts 'in which success or failure for major participants is critically dependent on computerized key activities along the path of events' (Demchak 2010), rather than expect activities solely in the virtual realm.

KEY POINTS

- The Gulf War of 1991 is considered to be the first of a new generation of conflicts in which mastering the information domain becomes a deciding factor. Afterwards, the information warfare/operations doctrine was developed in the US military.
- Increasing dependence of the military, but also of society in general, on information infrastructures made clear that information warfare was a double-edged sword. Cyberspace seemed the perfect place to launch an asymmetrical attack against civilian or military critical infrastructures.
- The US military tested its information warfare doctrine during the NATO operation 'Allied Force' in 1999. It was the first armed conflict in the Internet and was actively used for the exchange and publication of conflict-relevant information. Thereafter, the term 'cyber-war' came to be used for almost any type of conflict with a cyber-component.
- The discovery of a computer worm that sabotages industrial processes and was programmed by order of a state actor has alarmed the international community. Some experts believe that this marks the beginning of unrestrained cyber-war among states.
- Others think that highly unlikely and warn against an excessive use of the term cyber-war. Future conflicts between states will be fought in cyberspace, but not exclusively. One useful term for them is cyber(ed) conflicts.

KEY IDEAS 27.1 Presidential Commission on Critical Infrastructure Protection

Following the Oklahoma City Bombing, President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) to look into the security of vital systems such as gas, oil, transportation, water, telecommunications, etc. The PCCIP presented its report in the fall of 1997 (President's Commission on Critical Infrastructure Protection 1997). It concluded that the security, economy, way of life, and perhaps even the survival of the industrialized world were dependent on the interrelated trio of electrical energy, communications, and computers. Further, it stressed that advanced societies rely heavily upon critical infrastructures, which are susceptible to classical physical disruptions and new virtual threats. While the study assessed a list of critical infrastructures or 'sectors'—for example, the financial sector, energy supply, transportation, and the emergency services—the main focus was on cyber-risks. The PCCIP linked the cyber-security discourse firmly to the topic of critical infrastructures. Thereafter, CIP became a key topic in many other countries.

Reducing cyber-in-security

The three different discourses have produced specific types of concepts and countermeasures in accordance with their focus and main referent objects (see Figure 27.2), some of which are discussed later.

The common and underlying issue in all discourses is information assurance, which is the basic (technical) security of information and information systems. It is common practice that the entities that own a computer network are also responsible for protecting it (governments protect government networks, militaries only military ones, and companies protect their own, etc.). However, there are some assets considered so crucial to the functioning of society in the private sector that governments take additional measures to ensure an adequate level of protection. These efforts are usually subsumed under the label of **critical (information) infrastructure protection**.

In the 1990s, critical infrastructures became the main referent object in the cyber-security debate. Whereas critical infrastructure protection (CIP) encompasses more than just cyber-security, cyber-aspects have always been the main driver (see Key Ideas 27.1). The key challenge for CIP efforts arise from the privatization and deregulation of large parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put many critical infrastructures in the hands of private (transnational) enterprises. Market forces alone are not sufficient to provide the aspired-for level of security in designated critical infrastructure sectors,[1] but state actors are also incapable of providing the necessary level of security on their own (unless they heavily regulate, which they are usually reluctant to do).

Public–Private Partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as a panacea for this problem in the **policy community**—and cooperation programmes that follow the PPP idea are part of all existing initiatives in the field of CIP today, although with varying success. A large number of them are geared towards facilitating information exchange between companies and between companies and government on security, disruptions, and best practices (President's Commission on Critical Infrastructure Protection 1997: 20).

Information assurance is guided by the management of risk, which is essentially about accepting that one is (or remains) insecure: the level of risk can never be reduced to zero. Cyber-incidents are bound to happen because they simply cannot be avoided, even with perfect risk management. This is one of the main reasons why the concept of resilience has gained so much weight (Perelman 2007). Resilience is commonly defined as the ability of a system to recover from a shock, 'bouncing back' either to its original state or to a new

[1] The most frequently listed examples are banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply.

	Technical	Crime–espionage	Military/civil defence
Main actors	▪ Computer experts ▪ Anti-virus industry	▪ Law enforcement ▪ Intelligence community	▪ Security professionals, military, civil defence establishment
Main referent object	▪ Computers ▪ Computer networks	▪ Business sector ▪ Classified information	▪ Military networks, networked forces ▪ Critical infrastructures
Protection concept	Information assurance		
National level	▪ CERTs (specific for different domain, milCert, govCert, etc.)	▪ Computer law	▪ Critical (information) infrastructure protection ▪ Resilience ▪ Cyber-offence; cyber-defence; cyber-deterrence
International level	▪ International CERTs ▪ International information security standards	▪ Harmonization of law (Convention on Cybercrime) ▪ Mutual judicial assistance procedures	▪ Arms control ▪ International behavioural norms

Figure 27.2 Countermeasures

adjusted state. Resilience accepts that disruptions are inevitable and can be considered a 'Plan B' in case something goes wrong.

In the military and strategic discourse, the terms cyber-offence, cyber-defence, and cyber-deterrence are used. Under scrutiny, cyber-defence (and to some degree -offence) are very similar to information assurance practices, but the terminology signifies that military actors or the intelligence community are involved. Beyond this, increased feelings of insecurity have led to higher incentives for states to control the risk of escalation and conflict. As a result, the number of ministerial meetings and conferences has increased, and **norms** aiming to curb aggression in and through cyberspace are emerging. In particular, there are clear signs that powerful states like the US are working to build a specific deterrence regime for cyberspace. The considerable involvement of US officials in many of the international cyber-security governance processes is linked to its strategic interest in shaping international norms for behaviour in cyberspace (Stevens 2012), which will create more certainty about the costs (and benefits) of a cyber-attack.

In the same vein, the applicability of international law to the cyber-domain has also been discussed and partially settled. In 2013, a consensus emerged among several states, and at the UN, in the EU, and in NATO, that International Humanitarian Law (IHL) fully applies in cyber-operations. In parallel, several intergovernmental bodies confirmed the applicability of state sovereignty and the international norms and principles that flow from sovereignty. The most important questions with regard to *jus ad bellum*, that is, when a cyber-attack would be considered an armed attack by another state and how to react in that case, are discussed in the 'Tallinn Manual on the International Law Applicable to Cyber Warfare' (Schmitt 2013).

Yet, while states are seeking to ensure that the risk of escalation is reduced, they are unwilling to forgo offensive and aggressive use of cyberspace altogether. Solutions to control the use of computer exploitation through arms control or multilateral behavioural norms—agreements that might pertain to the development, distribution, and deployment of cyber-weapons, or to their use—are highly unlikely. Traditional capability-based arms control will clearly not be of much use, mainly due to the impossibility of verifying the technical capabilities of actors, especially non-state ones. The avenues available for arms control in this arena are primarily information exchange and confidence building, whereas structural approaches and attempts to prohibit the means of cyber-war altogether or restricting their availability are largely impossible due to the ubiquity and dual-use nature of information technology.

KEY POINTS

- There are a variety of approaches and concepts to secure information and critical information infrastructures. The key concept is a risk management practice known as information assurance, which aims to protect the confidentiality, integrity, and availability of information and the systems and processes used for the storage, processing, and transmission of information.
- Critical infrastructure protection (CIP) became a key concept in the 1990s. Because a very large part of critical infrastructures is not in the hands of government, CIP practices mainly build on public–private partnerships. At the core of them lies information sharing between the private and the public sector.
- Because the information infrastructure is persuasively insecure, risk management strategies are complemented by the concept of resilience. Resilience is about having systems rebound from shocks in an optimal way. The concept accepts that absolute security cannot be obtained and that minor or even major disturbances are bound to happen.
- The military concepts of cyber-defence and cyber-offence are militarized words for information assurance practices. Cyber-deterrence, on the other hand, is a concept that moves deterrence into the new domain of cyberspace.
- Internationally, efforts are underway to harmonize cyber-law. In addition, because future use of cyberspace for strategic military purposes remains one of the biggest fears in the debate, there are attempts to curtail the military use of computer exploitation through multilateral behavioural norms.

The level of cyber-risk: overstated?

Different political, economic, and military conflicts clearly have cyber(ed)-components. Furthermore, criminal and espionage activities with the help of computers happen every day. Cyber-incidents are causing minor and occasionally major inconveniences. These may be in the form of lost intellectual property or other proprietary data, maintenance and repair, lost revenue, and increased security costs. Beyond the direct impact, badly handled cyber-attacks have also damaged corporate (and government) reputations and have the potential to reduce public confidence in the security of Internet transactions and e-commerce if they become more frequent.

However, in the entire history of computer networks, there have been only very few examples of attacks or other type of incidents that had the potential to rattle an entire nation or cause a global shock. There are even fewer examples of cyber-attacks that resulted in actual physical violence against persons or property (Stuxnet being the most prominent). The huge majority of cyber-incidents have caused minor losses rather than serious or long-term disruptions. They are risks that can be dealt with by individuals or private entities using standard information security measures and their overall costs remain low in comparison to other risk categories like financial risks. Nonetheless, there is a clear shift towards a growing securitization and militarization of cyber-security as more and more states consider cyberspace as a strategic domain and open up 'cyber-commands', which are military units for cyber-war activities. This build-up of capabilities by state actors looks like an arms race in cyberspace. The uncertainty about the intentions of other states, and the practical inability to know whether such capabilities are offensive or defensive, lead to heightened feelings of insecurity.

More and more evidence is emerging that there is a high level of restraint in the use of cyber-tools in political conflict and that cyber-tools have limited use for coercion (Borghard and Lonergan 2017). Yet, the level of cyber-fears remains high and the military discourse has a strong mobilizing power. This has important political effects. The danger of overly dramatizing the threat manifests itself in reactions that call for military retaliation (as happened in the Estonian case and in other instances) or other exceptional measures. Although this chapter has shown how diverse the threat spectrum is and that there are many different types of countermeasures in place, this type of rhetoric invokes enemy images even if there is no identifiable enemy, favours national solutions instead of international ones, and centres too strongly on national security measures instead of economic and business solutions. In times of limited resources, governments have to be careful not to invest based on fears, but invest in efficient and pragmatic solutions that reduce the overall insecurity of information networks in peacetime.

On the one hand, the focus on regulating the behaviour of (other) states promises to have positive effects for cyber-security mainly by reducing the risk of escalation. At the same time, however, the recent focus on state-to-state relations and on state intervention is contested. Because cyberspace is a realm used by different actors for highly diverse activities, the security-seeking actions by states often directly clash with other uses and conceptions of cyberspace, social and economic. In particular, there are problems associated with the empowerment of intelligence and military establishments in matters of cyber-security. The military accumulation of cyber-capabilities in Western states is outpacing civilian comprehension and control. Similar problems hold true for intelligence agencies: while they may have the budget and technological resources that are best suited to respond to cyber-threats, their role also elicits great public unease. Public disquiet over government surveillance and cyber-capabilities could prove to be difficult for cyber-security strategies in the future.

KEY POINTS

- The majority of cyber-incidents so far have caused minor inconveniences and their cost remains low in comparison to other risk categories. Only very few attacks had the potential for grave consequences and even fewer actually had any impact on property. None have ever caused loss of life.
- Despite emerging evidence that cyber-tools might not be very effective in military operations, states consider cyberspace as a strategic domain and open up military units for cyber-war activities. This has started something like an arms race in cyberspace.
- The level of cyber-fears is high, with direct political consequences. Overstating the risk comes with the danger of prioritizing the wrong answers. Military solutions are given precedence over other solutions even though establishing cyber-security cannot be the task of the military in democratic states.

Conclusion

Despite the increasing attention cyber-security is getting in security politics and despite the possibility of a major, systemic, catastrophic incident involving critical infrastructures, computer network vulnerabilities are predominantly a business and espionage problem at the moment. However, a heightened sense of unease about the escalatory potential of cyber-conflict, fuelled by the certainty that more and more states are using cyberspace for strategic ends, has led state actors to attempt to (re)establish their authority in the virtual realm in the name of more security.

The trend is to invest in the old ways of stabilizing International Relations, focusing mainly on transparency measures and attempts to create deterrence effects through norm-building, ultimately coveting more order in cyberspace. This is currently giving rise to hopes for more stability, as the risk of escalation is reduced. Overall, indeed, it is clear that a secure, safe, and open cyberspace is not possible without the involvement and commitments of state actors. At the same time, however, states themselves remain the biggest threats to stability. State practices linked to cyber-exploitation are emerging as a major, if not biggest part of the problem, constantly creating more insecurity and hindering the removal of known insecurities. The main issue is that the normalization and stabilization efforts are geared towards a form of high-impact cyber-aggression that could indeed be devastating but that also has a low probability of occurrence. The biggest current issue, besides cybercrime, is cyber-exploitation: it is the world of intelligence communities, whose actions in home states are regulated by national law, but who are expected to act unfettered and without restraint in the international realm.

In seeking a prudent policy, threat representation must remain well informed and well balanced not to allow over-reactions with costs that are too high and benefits that are uncertain. For example, an 'arms race' in cyberspace, based on the fear of other states' cyber-capabilities, has detrimental effects on the way humankind uses the Internet. Also, solving the attribution problem would come at a very high cost for privacy. Even though we must expect disturbances in the cyber-domain in the future we must not expect outright disasters. Some of the cyber-disturbances may well turn into crises, but crisis can be managed. If societies become more fault-tolerant psychologically and more resilient overall, the likelihood of a catastrophe with lasting impact can be substantially reduced.

Cyber-security issues are also challenging for students and academics more generally. Recently, research focusing on the cyber-dimension of political conflict has started to appear more frequently in traditional strategic studies and International Relations journals. Using empirical data, it focuses on the familiar aspects of strategic interaction in (dyadic) conflict settings, asking how and to what degree cyberspace as a domain of warfare influences (inter alia) coercion, offence-defence theory, and deterrence. Given the particular ontological and epistemological choices of this research, it needs reliable data about cyber-incidents. These data needs lead to a bias for cyber-incidents that are known and create 'visible' or measurable effect—most of the incidents in the datasets are DDoS-attacks. However, these types of attacks are only a small part of the whole cyber-threats picture and arguably not the most important one. For Security Studies, looking at cyber-security in and through the representations of various actors in the political domain remains an important alternative. What is needed is more research focusing on the contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat.

? QUESTIONS

1. Who benefits in what ways from calling malware cyber-weapons?
2. What are the pros and cons of abolishing anonymity (and therefore partially solving the attribution problem) on the Internet in the name of security?
3. What side effects does the indiscriminate use of the term cyber-war have?
4. Are hacktivism activities a legitimate way to express political or economic grievances?
5. What are the limits of traditional arms control mechanisms applied to cyber-weapons?
6. Why does the intelligence community not have more information on the cyber-capabilities of other states?
7. What are the similarities and what the differences between information security and national security?
8. Which aspects of cyber-security should be considered a part of national security, and which aspects should not? Why?
9. What might be the next referent object in the cyber-security discourse?

FURTHER READING

- Arquilla, J. and Ronfeldt, D. F. (eds) (1997), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND. This is one of the earliest key texts about information warfare.
- Brown, K. A. (2006), *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, Arlington, VA: George Mason University Press. Provides a comprehensive overview of the evolution of critical infrastructure protection in the USA.
- Deibert, R. J. (2013), *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland & Stewart. An account of how the web has changed us—and what is currently changing in the web as powerful agents take control, with considerable consequences for citizens.
- Dunn Cavelty, M. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge. Examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda in the USA.
- Healey, J. (ed.) (2013), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Arlington, VA: Cyber Conflict Studies Association. A history of cyber-conflict, with a focus on power-politics.
- Libicki, M. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND. Explores the specific laws of cyberspace and uses the results to address the pros and cons of counterattack, the value of deterrence and vigilance, and other defensive actions in the face of deliberate cyber-attack.
- National Research Council (2009), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC: The National Academies Press. Focuses on the use of cyber-attack as an instrument of US policy and explores important characteristics of cyber-attack.
- Valeriano, B. and Maness, R. C. (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, New York: Oxford University Press. How 'real' is cyber-war? This book challenges the conventional wisdom that cyber conflict is substantially changing the nature and tactics of international interactions.

IMPORTANT WEBSITES

- **http://cipp.gmu.edu** George Mason University (GMU), Critical Infrastructure Protection (CIP) Program Website: the GMU CIP program is a valuable source of information for both US and international CIP-related issues and developments.
- **http://www.schneier.com** Schneier on Security: Bruce Schneier is a refreshingly candid and lucid computer security critic and commentator. In his blog, he covers computer security issues of all sorts.
- **http://www.iwar.org.uk** The Information Warfare Site: an online resource that aims to stimulate debate on a variety of issues involving information security, information operations, computer network operations, homeland security, and more.
- **http://www.infowar.com** Infowar Site: a site dedicated to tracking open source stories relating to the full spectrum of information warfare, information security, and critical infrastructure protection.

Visit the online resources that accompany this book for lots of interesting additional material: www.oup.com/uk/collins5e/