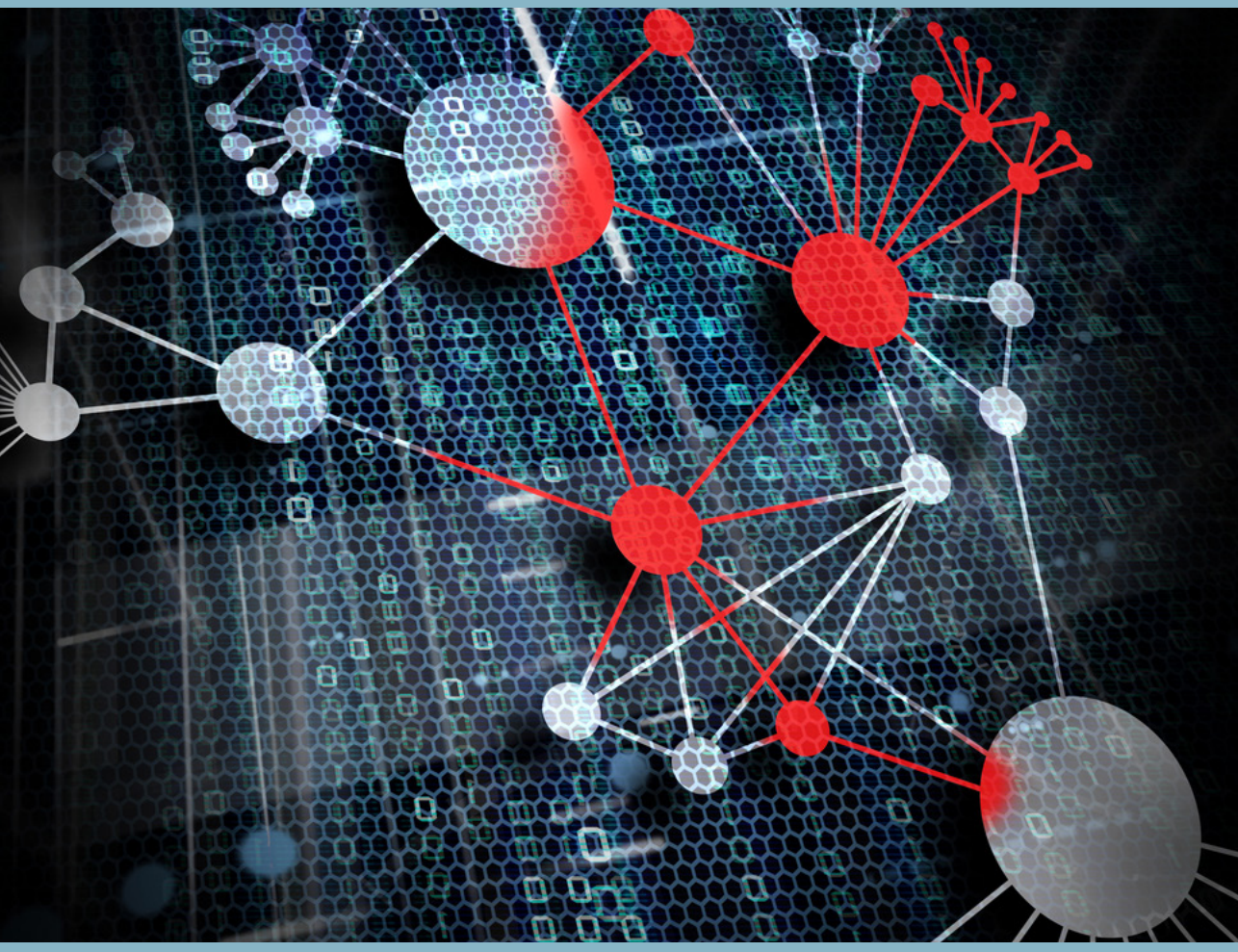
hoffmann

Bedrijfsrecherche - Consultancy & Opleidingen - ICT-Security

The Hague Centre for Strategic Studies

ASSESSING CYBER SECURITY

A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS



The Hague Centre for Strategic Studies

SECURITY

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

This report is part of the HCSS theme SECURITY. Our other themes are RESOURCES and GLOBAL TRENDS.

SECURITY

HCSS identifies and analyzes the developments that shape our security environment. We show the intricate and dynamic relations between political, military, economic, social, environmental, and technological drivers that shape policy space. Our strengths are a unique methodological base, deep domain knowledge and an extensive international network of partners.

HCSS assists in formulating and evaluating policy options on the basis of an integrated approach to security challenges and security solutions.

ASSESSING CYBER SECURITY

A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS

The Hague Centre for Strategic Studies (HCSS)

ISBN/EAN: 978-94-92102-12-6

Authors: Maarten Gehem, Artur Usanov, Erik Frinking, Michel Rademaker

The authors would like to thank TNO for its extensive input on chapter 3, and our Assistant Strategic Analysts (HCSS Internship Program) Jacques Mukena, Nicolas Castellon, Katarina Kertysova and Kelsey Shantz for their assistance in writing this report.

This report was made possible by funding and feedback from six organizations:
Hoffmann Bedrijfsrecherche BV, Capgemini, Netherlands Organization for Applied Scientific Research (TNO), The NLnet foundation, Municipality of The Hague

Graphic Design Studio Maartje de Sonnaville, The Hague
Print de Swart
Graphics Joris Fiselier

The Hague Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL

ASSESSING CYBER SECURITY

A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS

The Hague Centre for Strategic Studies

TABLE OF CONTENTS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world. In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. This report aims to help in this task by assessing what we know about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years. It answers the following questions: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?

Reporting is fragmented

The focus of the examined reports differs widely. Some reports look at all possible cyber attacks, others zoom in on specific threats such as Distributed Denial of Service attacks or malware. Some reports focus on a specific sector, or one country, others have a global scope. Methodologies used by the reports are often inconsistent and sometimes opaque: some are based on self-reporting (e.g., surveys), while others use data generated by software. One of the main observations of our study is that the range of estimates in the examined investigations is so wide, even experts find it difficult to separate the wheat from the chaff.

This leads to the conclusion that, although there is no shortage in the number of reports, well defined and comparable cyber threat data and risk assessments are missing.

Threat assessment

In general, the number of registered cyber attacks is on the rise, partly due to an increase in cyber activity and reporting itself, with estimates of the growth in the number of cyber attacks ranging from a few percent to a tenfold increase. Most of these attacks are motivated by criminal, financial intent. There also seems to be a rise in espionage incidents. The picture furthermore differs per type of attack: in 2013, over a quarter of all cyber crime activities emanated from computers in the US, according to Symantec. And an assessment by Verizon suggests that almost half of all cyber espionage activities come from East Asia. The exact identity of who is behind these attacks remains unclear.

Most of the attacks originate from outside organizations, although many reports note that a sizable share of the attacks is conducted with help from current or former employees, ranging from 6 to 28% of all attacks. Governments, together with the financial sector and industry, stand out as main targets.

There is agreement on the fact that the costs of cyber attacks are significant. Most reporting focuses on larger companies (e.g., with over 500 employees). Existing estimates point to significant costs, which rise per person per organization in parallel to company size. On a national level, this leads to significant losses. McAfee estimates that the average loss due to cyber attacks amounts to over 0.8% of GDP annually, with the Netherlands and Germany topping the chart with over 1.5%. However, the range of estimates is large.

Trends in cyber security

We highlight three trends that point to the changing nature of perpetrators. First, a new cyber crime economy is on the rise. An expanding zero-day exploit market increases the vulnerability of a large share of users. Second, state actors and organized criminal groups are converging capabilities: state actors are increasingly hiring such groups as 'cyber-mercenaries'. Third, because states are rapidly developing offensive capabilities, the threat of cyber weapons becoming a major ingredient in warfare is increasing.

As for targets, increasing interdependencies, partly due to the advent of the Internet of Things (IoT), are leading to cascading risks. Big Data hosting companies and digital certificate providers have become a focal point for attacks. In addition, our IDs are more and more the target of attacks, with perpetrators focusing more on 'who you are' than 'what you own'. Finally, GPS positioning, navigation, and timing stand out as a 'weak link' in critical systems.

Countering cyber attacks is becoming more difficult because perpetrators have expanding options available. Increasing availability of anonymization and abuse of Big Data analytics has helped to create a thriving cyber crime industry providing data and software for almost any type of cyber attack on a commercial basis. Even encryption might no longer be able to compete with the vastly improved computing power combined with backdoors in software. Finally, cyber attacks are taking place out in the open but camouflaged: increasingly, legitimate acts will become a means to gain an unfair advantage through cyber attacks.

Responses to cyber risk factors

More and more nations see cyber security as a serious issue as evidenced by their development of national cyber strategies. However, several countries have still to develop or publish a strategy on cyber security. Another indicator of the rising importance of cyber security in the public and private sector, is rapidly growing spending of cyber security hardware, software and services.

Our meta-analysis of five rankings of cyber security at the national level indicates that the Netherlands, UK-, and the US are noted as best prepared and protected. These countries are followed by Japan, Germany, Finland, Canada, Australia, South Korea and Sweden.

General recommendations

The picture that emerges from our meta-assessment of cyber threat analyses is one where it has become difficult to see the forest for the trees. There are clearly a lot of reports around, but definitions and methods are difficult to compare. If we want to provide a more encompassing and comparable assessment of cyber threats, and create greater awareness thereof, we should:

- In line with emerging efforts on the international level[1], develop shared, commonly agreed definitions, metrics-, and reporting standards to enhance threat assessments. This will provide more targeted investments in cyber security, on both company and government level.
- Anticipate trends and developments in an early stage to include potential new threats.
- Develop evidence-based cyber security policies that rely more on data and indicators, rather than subjective perceptions.
- Consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.

INTRODUCTION

INTRODUCTION

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign that the seriousness of cyber attacks for organizations, both public and private, and citizens all over the world, is getting more recognition and attracts more attention from media and experts. Research can help better understand the seriousness of cyber threats and pave the path to improved prevention, mitigation, and resilience. But the range of estimates in these reports is so large, even experts find it difficult to separate the wheat from the chaff.

This report investigates the aggregate picture that emerges from these reports. We collected around 70 studies that were published by CERTs, security companies, and research organizations from 15 countries from the last few years. In three chapters, we look at what these reports say about the threats in cyber space. Chapter 2 gives a quantitative overview of cyber attacks. It focuses on the reporting itself, the general trends, perpetrators, targets, tools and techniques used, and their impact. Chapter 3 looks at some new trends mentioned in these reports, and gives a (non-exhaustive) overview of some trends that can help broaden our 'cyber threat horizon'. In chapter 4, we zoom in on the responses to these threats from the private and public sector, and the public. Do we see gaps in the assessment of threats, and focus of the strategies in place? A final chapter lists the main conclusions of this report, with recommendations for the future.

1.1 Some terminological clarifications

What's in a name? Attacks, incidents, breaches – the reports we collected use a variety of terms related to the field of cyber security. Four of these terms, listed below, are particularly important:

- Attack: A malicious act that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself. [2]
- Incident: A security event that compromises the integrity, confidentiality, or availability of an information asset. [3]
- Breach: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.[4]
- Disclosure: A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.[5]

In addition, a glossary of terms and definitions used in this report is available in Annex 4.

2 COMPARING CYBER THREAT ASSESSMENTS

2 COMPARING CYBER THREAT ASSESSMENTS

This chapter provides a quantitative assessment of cyber threats. First, we examine the reporting itself. Do the studies show a specific geographical focus? From what organizations do they come? What is the focus of their analysis? Second, we look at the grand trend in the incidents reported. Next, we zoom in on perpetrators. What motivates them? Where do they come from? A fourth section looks at tools and techniques that were used. The final section of this chapter focuses on victims: where were they located? What was their profile? How were they impacted by cyber attacks?

This chapter is based on the following categorization of cyber threats:

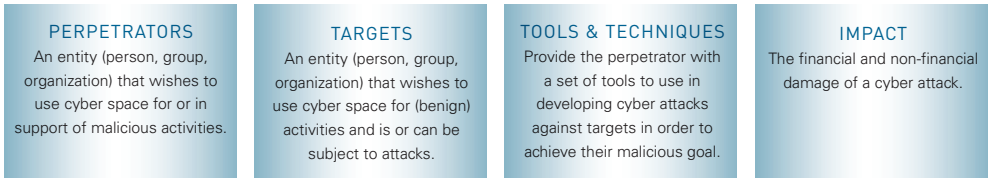


FIGURE 1 OVERVIEW OF CYBER THREAT CATEGORIZATION

2.1 Reporting is fragmented

The corpus of studies shows a fragmented picture. Some studies look at threat trends, summarizing cyber attacks of the last year, others are forecasting key developments in the next. Some focus on specific sectors and industries, such as banks or hospitals. Others zoom in on attacks in one country, like national Computer Emergency Response Teams (CERT) trend reports. Some reports look at specific types of attacks, like data breaches or malware. Researchers use different methods to acquire their information – from surveys to reports of actual attacks. From all these different perspectives and approaches, it is not easy to see the woods for the trees. We therefore begin in this section by providing a bird's-eye view of our findings, summarizing key factors, such as: years reported, types of organization, home-country origins, and geographical

focus of analysis. The open source reports we gathered look at 2013 or 2014, with some including data for preceding years as well.

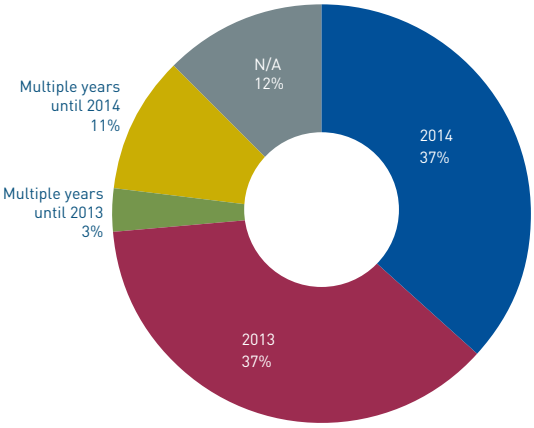


FIGURE 2 STUDIES ON CYBER THREATS ACCORDING TO YEAR(S) OF ANALYSIS

Studies come from a broad range of organizations.[6] Most (57%) are published by private organizations, such as software companies like IBM, or security providers like Symantec, McAfee and Kaspersky. About a quarter originates from governmental sources, such as Computer Emergency Response Teams (CERTs) or EU-bodies. The remainder (almost one-fifth) comes from research organizations (think tanks and academic institutions) and one non-for-profit organization (i.e., the World Economic Forum).

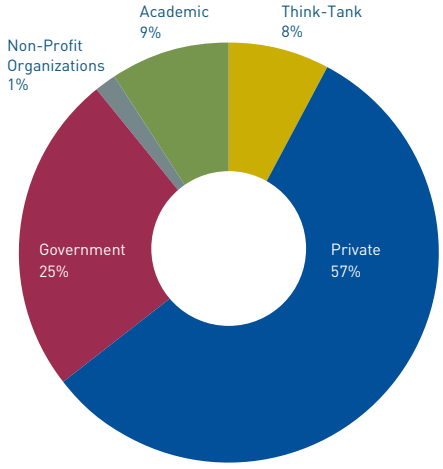


FIGURE 3 ANALYZED STUDIES ON CYBER THREATS ACCORDING TO TYPE OF ORGANIZATIONS

To a large extent, the body of reports published comes from US-based organizations. About one-third comes from other European countries or European organizations. 15% of studies are from other, non-European countries.

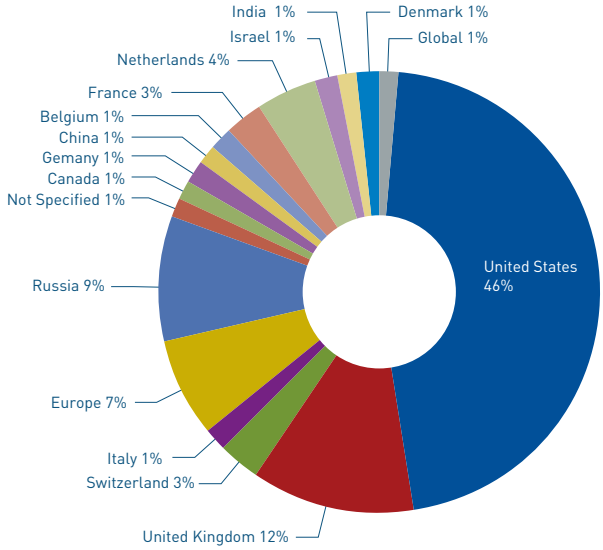


FIGURE 4 ORGANIZATIONS BASED ON COUNTRY

Most reports have a global focus. Reports with a national focus are predominantly CERT publications or other publications by national governments.

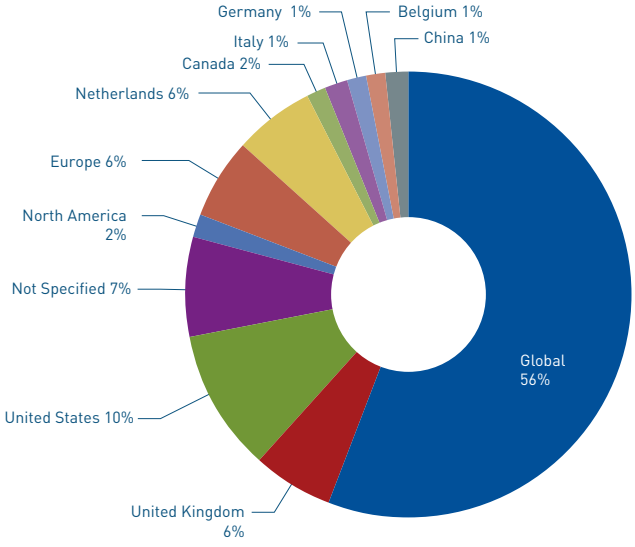


FIGURE 5 GEOGRAPHICAL FOCUS OF ASSESSED CYBER THREAT STUDIES

2.2 Increasing cyber incidents reported

One thing almost all reports agree on: cyber attacks are on the rise. IBM estimates that the average company experienced 109 security incidents in 2013, i.e., those attacks large enough to be considered a real cause of concern (see Figure 6). This represents an increase of 19 from the year before. The number of attacks caused by malicious actors aiming to collect, disrupt, deny, degrade or destroy information system resources or the information itself is estimated to be around 17,000 – a fraction of all security events (that is, "an event on a system or network detected by a security device or application").[7]

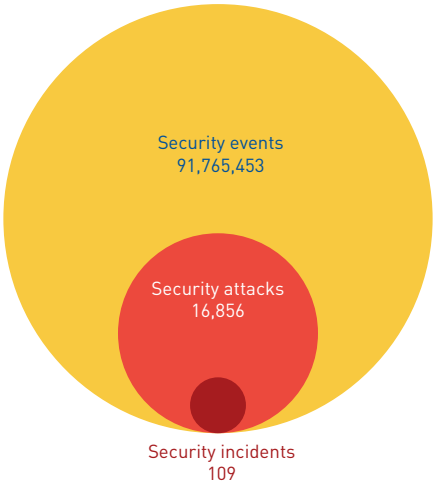


FIGURE 6 AVERAGE CYBER SECURITY EVENTS, ATTACKS AND INCIDENTS EXPERIENCED PER COMPANY IN 2013, FROM A SAMPLE OF NEARLY 1,000 OF IBM CLIENTS IN 133 COUNTRIES (IBM, 2014)

The total number of cyber incidents is difficult to assess, but one report, based on a survey of almost 10,000 security, IT, and business executives, suggests a 13-fold increase since 2009, to almost 45 million reported cyber incidents in 2014 (see Figure 7).

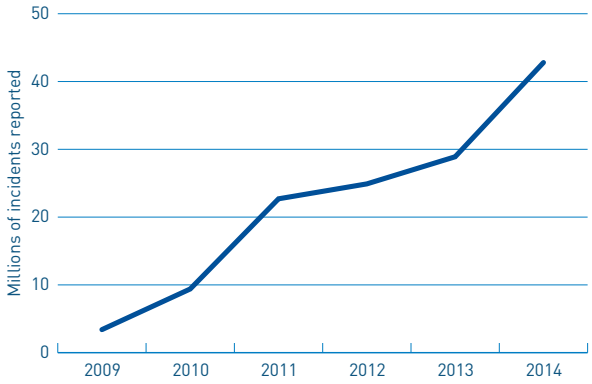


FIGURE 7 CYBER INCIDENTS REPORTED PER YEAR, BASED ON A SURVEY OF OVER 9,700 SECURITY, IT- AND BUSINESS EXECUTIVES AROUND THE WORLD (PWC, 2015)

Human Error

IBM notes in its Cyber Security Intelligence report from 2014 that in over 95% of incidents, human error is a contributing factor–from poor password protection to using an unsecured internet connection. A recent publication by Hoffmann Bedrijfsrecherche B.V., a Dutch fraud investigation bureau, notes that due to such negligence, security tests are able to penetrate three out of four companies.[8] Five security flaws stand out: predictable passwords; unused servers connected to the internet; website weaknesses; available but forgotten, 'old data', such as back-ups and source codes; lacking use of security protocols.

National Computer Emergency Response Teams (CERTs) also signal a steady, albeit less steep, increase in the number of reported incidents (see Figure 8). In India, the total number of incidents reported rose from around 10,000 in 2010 to over 70,000 in 2014 – a sevenfold increase. In Belgium, reported incidents increased by a similar factor: from 1,389 in 2010 to 9,866 incidents reported in 2014. US-CERT data, which only shows incidents reported by federal agencies, indicates a more moderate increase from around 40,000 in 2010 to over 67,000 in 2014. CERTs in China and Denmark show increases of 50 to over 200% respectively.

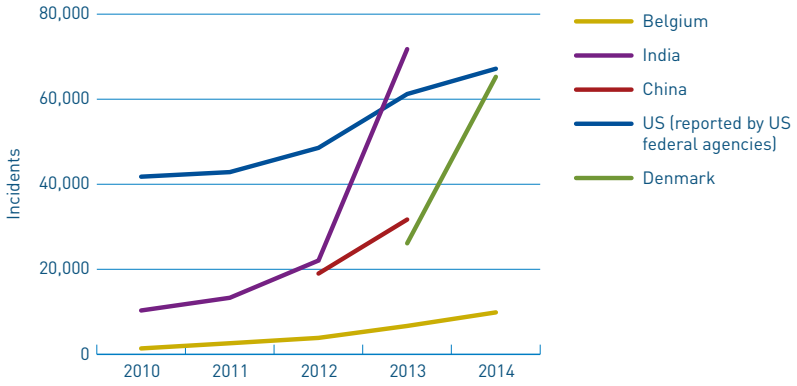


FIGURE 8 NUMBER OF REPORTED OR HANDLED INCIDENTS BY COMPUTER EMERGENCY READINESS TEAM (CERTS) IN FIVE COUNTRIES (BE-CERT, 2015; INCERT, 2015; CN-CERT, 2013, 2014; ICS-CERT, 2014; DKCERT, 2015).

Note that the numbers do not represent the total incidents per country in a specific year. Much of these figures reflect ease of and sensitivities around reporting. What is considered as a cyber attack differs per CERT. For example, China does not consider scanning attempts as cyber attacks, whereas Belgium and Denmark do (see also paragraph 2.4). In addition, the US figures represent reported incidents by governmental organizations.

A note on rising cyber security incidents

It is difficult to state the exact increase in actual incidents. First, the number of ICT devices and infrastructures has rapidly increased. So too has the amount of data created, replicated, and stored. The 'digital universe' is set to double year on year. Annually generated data is expected to rise from 130 exabytes in 2005, to 40,000 exabytes (400 trillion gigabytes) by 2020 (see Figure 8B).[9]

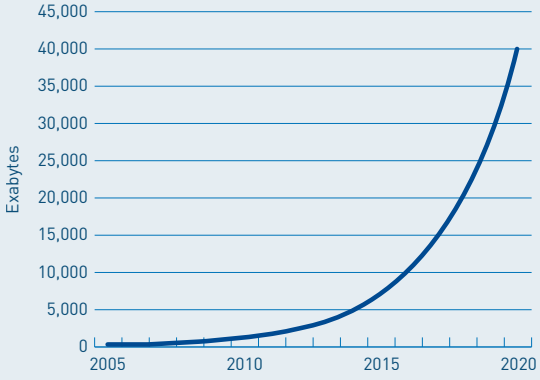
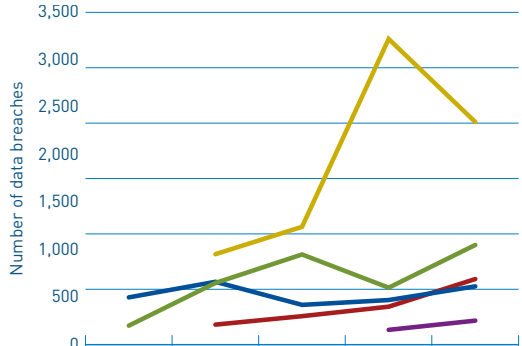


FIGURE 8B EXPONENTIAL GROWTH OF THE DATA UNIVERSE

The opportunities are tremendous. Communication networks, including the internet, and digitally stored information are used to execute and coordinate political, economic, scientific and social operations and services, from electronic transportation cards to the Arab Spring. Large amounts of classified, confidential and personal data are stored on millions of servers connected to the internet. In our day-to-day life we all rely on such data making purchases in a supermarket, making phone calls, sending e-mails, ordering goods from an online store or booking flights and hotels. This data can allow smooth use of all these and many other services. But there is a downside to these benefits too. Our data is a boon for criminals, terrorists, hacktivists, and intelligence agencies worldwide.

Second, the rising trend of incidents will likely reflect an increase in reporting itself, due to heightened awareness, opportunities to report attacks safely, and legislation obliging organizations to do so. At the same time, many incidents will not be reported – the exact number of incidents and breaches is thus much larger. There are some indications that less than half of all attacks are actually reported.[10]

If we zoom in on those attacks that most people associate with cyber threats, data breaches, or the intentional or unintentional release of secure information to an untrusted environment, we see a similar rising pattern (see Figure 9). In five reports by private companies that investigate data breaches, we see an upward trend over the last few years.



	2009	2010	2011	2012	2013
Verizon	200	650	950	600	1,050
III	498	662	419	470	614
Trustwave		211	300	400	691
Symantec				156	253
Risk Based Security		953	1,241	3,220	2,345

FIGURE 9 NUMBER OF DATA BREACHES, AS MEASURED BY VERIZON, III, TRUSTWAVE, SYMANTEC, AND RISK BASED SECURITY (2009-2013)

2.3 Perpetrators

2.3.1 Motivation

We may worry about 'Cyber Armageddon', or some other form of apocalyptic catastrophe destroying ICT infrastructures, but studies investigated point to small-scale criminal attacks as being the most common. Sophisticated Advance Persistent Threats (APT) that are conducted over a long time frame are rare. Instead, cyber attacks aimed at financial gain are judged to be the most frequent form of illegal cyber activity according to three reports (see Figure 10).

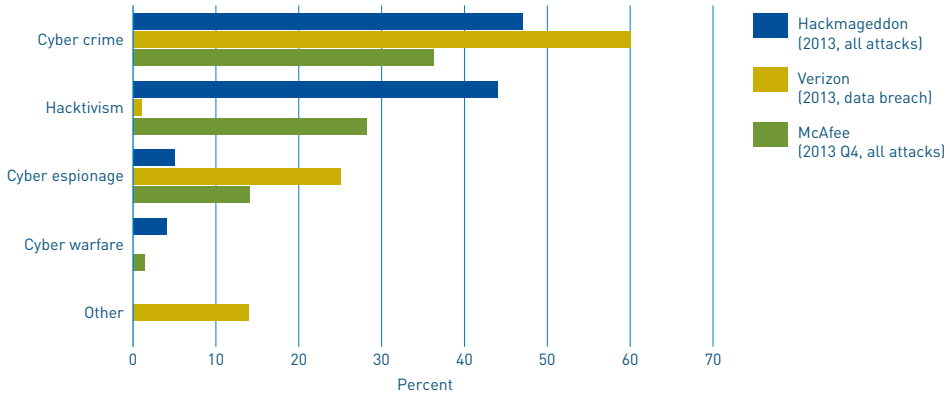


FIGURE 10 TYPE OF CYBER ATTACKS ACCORDING TO MOTIVATION , DISTINGUISHING CYBER CRIME, HACKTIVISM, CYBER ESPIONAGE, CYBER WARFARE, AND 'OTHER', IN 2013 (MCAFEE 2014; VERIZON 2015; HACKMAGEDDON.ORG.ORG 2015)

Most attacks are motivated by criminal, particularly financial intent. Attacks of an activist nature seem to be less common, but estimates vary widely – from over 40% to only a few percent. Espionage includes both the economic and politically motivated espionage, and seems to be on the rise, according to Verizon. Hackmageddon.org also notes an increase in cyber from 5 % in 2013 to 10% in 2014.

Cyber crime as a service

Increasingly, organized crime groups (OCGs) are resorting to cyber criminal activities. Online fraud shows a serious "return on investment" and good value for money compared to other types of crime. Where OCGs do not possess the capability to perform cybercrime activities on their own, they hire skilled people or buy their services, also known as 'cyber crime as a service'. This is partly influenced by the emergence of virtual currencies, such as Bitcoin. This opens up a new payment system to exchange goods or services. In addition, the large increase in

use of virtual currencies has created new targets for perpetrators in itself.[11] The attack of Mt. Gox, a Bitcoin exchange, in 2014 probably marks a new age of bank robbing and online theft.[12]

2.3.2 Location of attackers

Where are the attackers located? Most attacks emanate from outside the organization, but the concern for insider attacks is substantial: between 6 and 28% of attacks surveyed came from within organizations (see Figure 11).

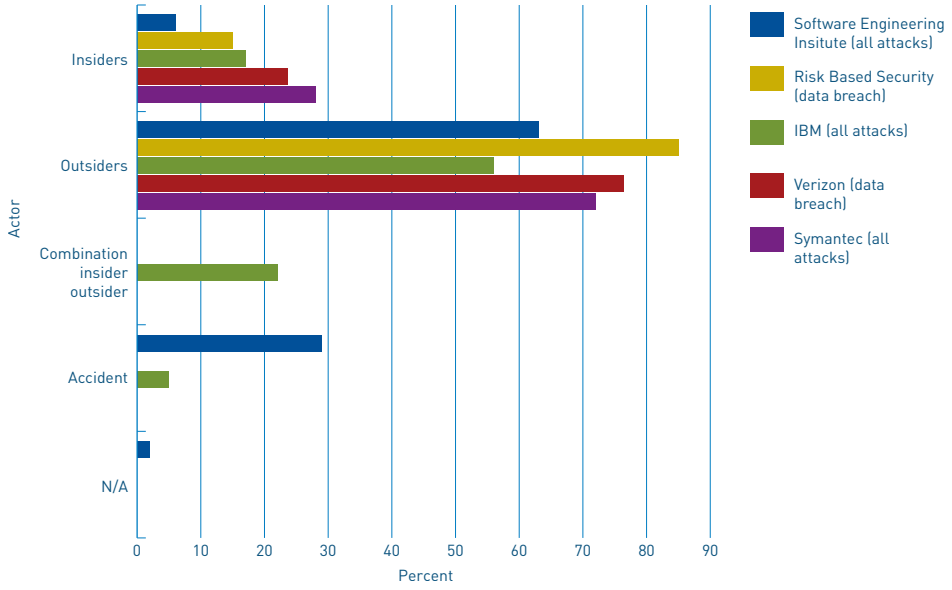


FIGURE 11 INSIDER VS. OUTSIDER THREATS IN 2013, ACCORDING TO SYMANTEC (ALL ATTACKS), IBM (ALL ATTACKS), VERIZON (DATA BREACH) AND RISK BASED SECURITY (DATA BREACH) (ALL STUDIES PUBLISHED IN 2014)

Attempts to locate perpetrators of these attacks are clouded by the 'problem of attribution': an attack comes with very little, if any, traces of who did it. Even the biggest intelligence agencies find it difficult to pinpoint the perpetrators responsible. Yet some attempts have been made to locate the IP addresses that attacks were launched from. These assessments point to countries with the highest number of internet users: China and the US (see Figure 12). Russia, Taiwan, Germany, and South Korea are also, albeit to a much smaller extent, mentioned. Yet, there is considerable disagreement in both the weight per country, as to what countries hosted most IP

addresses responsible for attacks (note, for example, the diverging scores for Nigeria and Indonesia). These differences are largely because of the number of cases investigated: 691 cases (Trustwave) and an unspecified number (Akamai). In addition, the reports have a somewhat different focus in the attacks investigated: the Trustwave report looks at data breaches, Akamai focuses on online cyber attacks. Finally, these reports measure attack activity of people and organizations using services provided by the company itself.

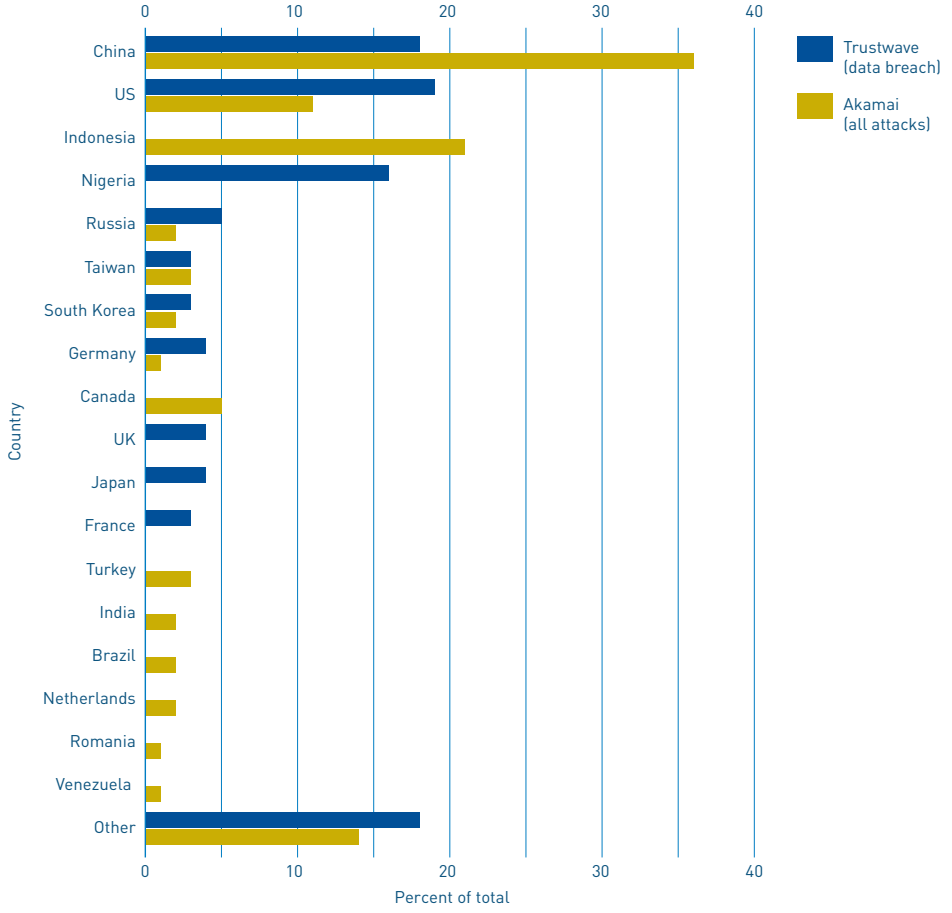


FIGURE 12 COUNTRY WHERE IP ADDRESS OF ATTACK IS LOCATED, ACCORDING TO TWO REPORTS, IN 2013 (AKAMAI 2013 Q1-4; TRUSTWAVE 2014). MORE PRECISE ATTRIBUTION OF THE ACTOR AND ITS LOCATION IS OFTEN IMPOSSIBLE. ATTACKS MAY BE ROUTED VIA A SERVER IN THE NETHERLANDS, BUT THE ACTOR ITSELF MAY SIT BEHIND A COMPUTER ON THE OTHER SIDE OF THE WORLD. THIS PICTURE THUS DOES NOT NECESSARILY SHOW THE LOCATION OF ATTACKERS.

It seems that computers in China and the US are used most frequently for hosting attacks, and this is partly confirmed by an earlier assessment of data breaches in 2012 (Figure 13). This assessment also shows that the picture may differ depending on the type of attack. According to this assessment, espionage is emanating mostly from China, whereas attacks coming from countries like Russia, Bulgaria and Romania are almost all criminal in nature.

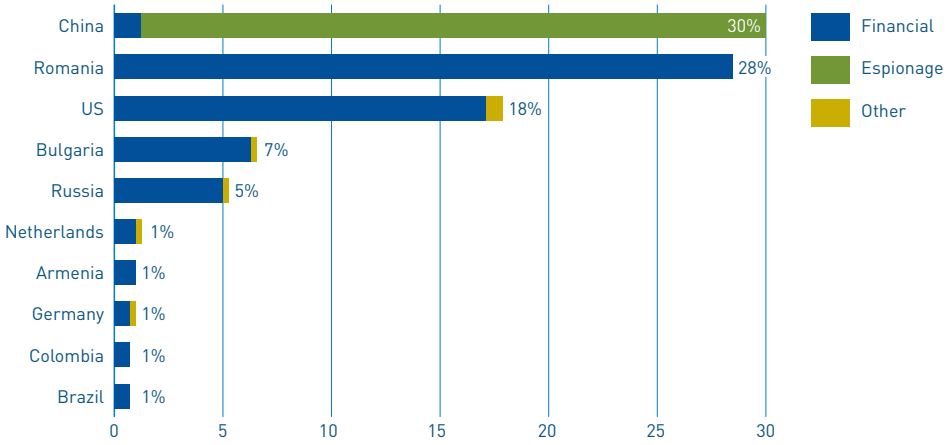


FIGURE 13 ORIGIN OF DATA BREACHES, DIFFERENTIATED BY MOTIVATION (2012) (VERIZON, 2013)

Cyber espionage

Espionage attacks seem to originate predominantly from East Asia, most notably China, and Eastern Europe, specifically Russia (see Figure 14). And as Figure 15 illustrates, these attacks are mostly geared at US actors and some East Asian countries (South Korea, Japan, Vietnam and the Philippines).

Such espionage attacks can be attributed to foreign governments, commercial organizations and organized criminal groups alike. All these groups use cyber espionage activities to steal valuable information or to increase their intelligence position. In addition, governments, being generally the more advanced perpetrators, continue to evolve their tools, techniques and procedures to avoid detection and reduce a forensic footprint of their activities in a victim's infrastructure.[13] Although organizations subject to many cyber espionage activities are making some gains in protection against such attacks, perpetrators still have a free reign in breached environments for a long time before being detected. In 2014, espionage was detected on average after 205 days in 2014 (compared with 229 days in 2013).[14]

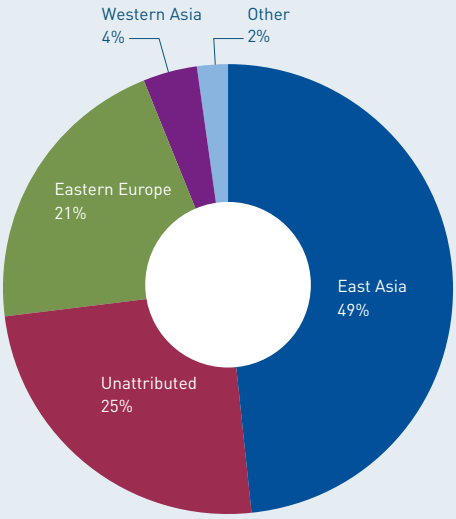


FIGURE 14 ORIGIN OF DATA BREACHES AIMED AT ESPIONAGE IN 2013, ACCORDING TO VERIZON, BASED ON 227 DATA BREACHES (VERIZON, 2014)

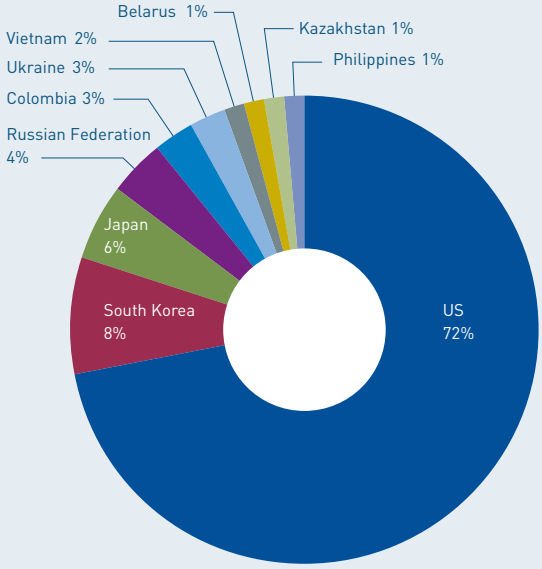


FIGURE 15 TARGET COUNTRIES OF DATA BREACHES AIMED AT ESPIONAGE IN 2013, BASED ON 227 DATA BREACHES (VERIZON, 2014)

For cybercrime activities, Symantec points to the US as both the origin and the predominant target of attacks (see Figure 16).

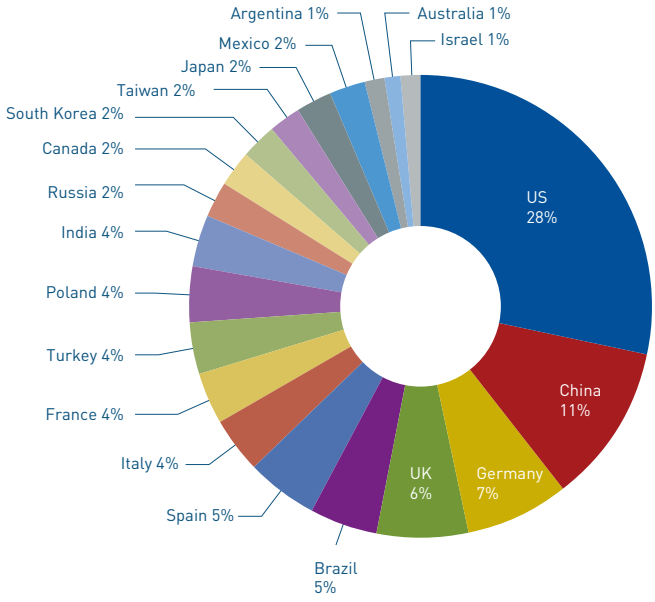


FIGURE 16 TOP 20-COUNTRIES GENERATING CYBER CRIME[15]

2.4 Tools and techniques

What tools and techniques were used by perpetrators? Many reports investigate the methods malicious actors use to disrupt, destroy or otherwise misuse data. There is a lot of variability in the type of tools these reports focus on, and the way they classify them. Figure 17 shows that four out of five organizations point to malware as most prevalent. But overall, there is a wide difference in assessments of what tools and techniques are actually most used and worrisome.

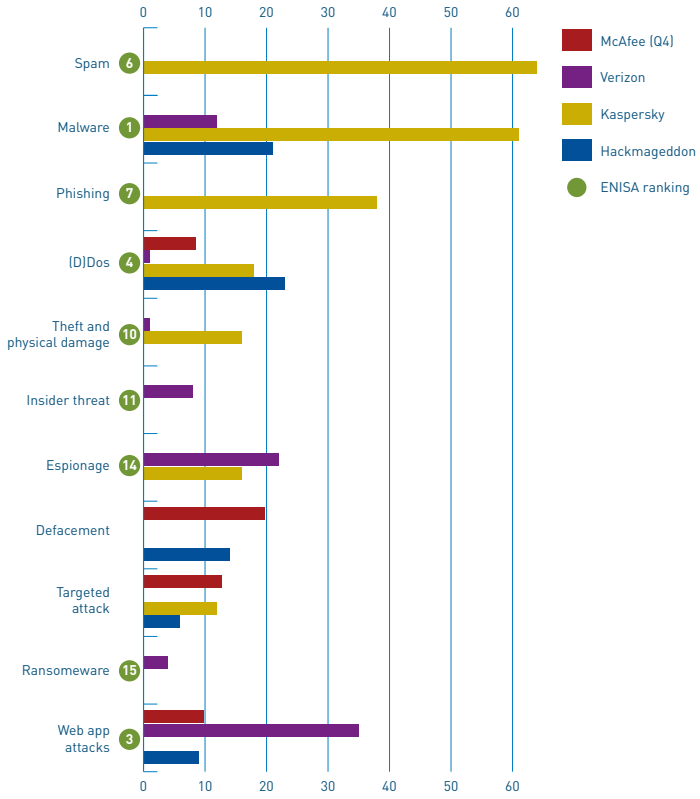


FIGURE 17 TOP CYBER ATTACK TOOLS AND TECHNIQUES USED IN 2013 ACCORDING TO MCAFEE, VERIZON, KASPERSKY, HACKMAGEDDON.ORG, AND ENISA (2014). THE ENISA REPORT IS A META-ANALYSIS OF RISK ASSESSMENTS ITSELF AND GIVES A TOP-15 OF MOST WORRISOME ATTACK TECHNIQUES. THESE ARE REPRESENTED BY THE GREEN NUMBER IN THE CHART, WITH 1 BEING THE MOST WORRISOME THREAT.

The differences in focus are also apparent when looking at threat assessments by governmental CERTs. Figure 18 shows the diverging focus of tools and techniques specified. Malware, (D)Dos attacks and Spam/Phishing are reported by all CERTs, and vulnerability reporting by three out of four. And again, malware attacks are considered most prevalent. But apart from that, there are big differences in how CERTs categorize tools and techniques used. For example, Denmark singles out copyright issues, while Belgium looks at 'system incidents', such as infected web servers. Although this is difficult to assess, the varying scores per country are likely to reflect national differences to some extent. But they also reflect the focus of CERTs themselves. The data for China, for example, indicates a strong focus on phishing incidents, with over a third of handled incidents in that category (in this case, all incidents under the Spam/Phishing category concern 'phishing'). And although not reported as such, it is likely

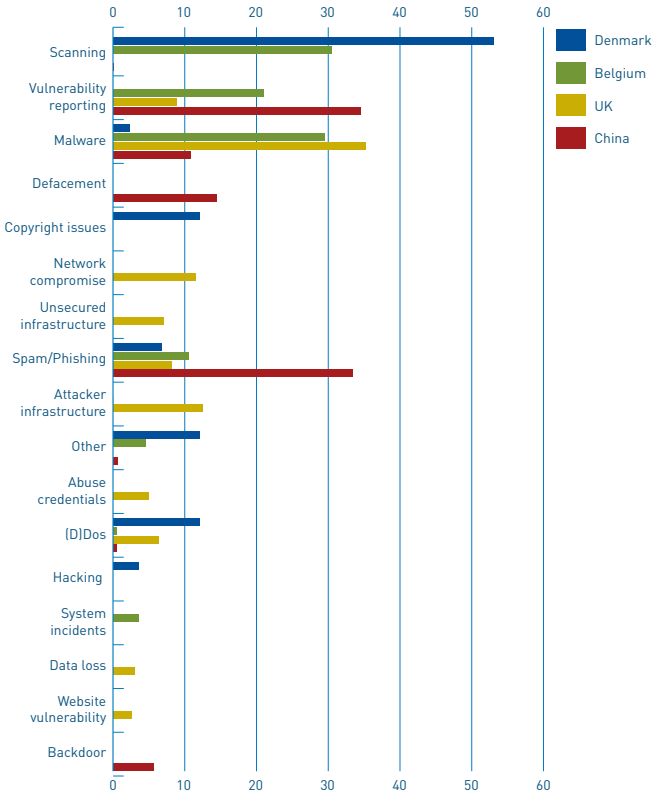


FIGURE 18 TOP CYBER ATTACK TOOLS AND TECHNIQUES USED IN 2013 AND 2014 ACCORDING TO CERTS OF CHINA (INCIDENTS HANDLED), UK (REPORTED), BELGIUM (REPORTED) AND DENMARK (REPORTED). (BE-CERT, 2015; CN-CERT, 2014; UK-CERT, 2014; DKCERT, 2015)

that in both China and the UK, scanning of websites was frequent, as is apparent in the statistics from Belgium and Denmark.

Increasingly severe DDoS attacks

DDoS are a popular weapon of choice since they provide anonymity to the attacker.[16] And with the expanding number of computers available, and increasing speeds of internet connections, DDoS attacks are also expected to continue to increase in bandwidth. The severity of DDoS attacks has increased significantly over the last years. Whereas the bandwidth of the largest attack in 2003 was still around 1 Gigabytes per second (Gbps), in 2013 it factored at approximately 309 Gbps. DDoS attacks are also being used as a decoy of performing the actual breach in a victim's infrastructure.

2.4.1 Malware

As the previous paragraph points out, malware is one of the most prevalent attack techniques being used. Some reports point to the emergence and rise of a do-it-yourself malware market, commonly referred to as 'Malware-as-a-Service' (MaaS). Similar to legitimate commercial software companies, criminal malware providers offer malware services and support to ill-intended actors. Increasingly, MaaS is becoming a component of the underground economy.[17]

Because of such developments, malware is increasing. Three reports that investigate the origin of malware attack point to the US, Russia, Germany and the Netherlands as dominant sites for malware hosting. Again, note that attacks may be routed via a server in a country where the attacker does not reside: an IP address in the US may be used, but the actor itself may sit behind a computer in Europe.

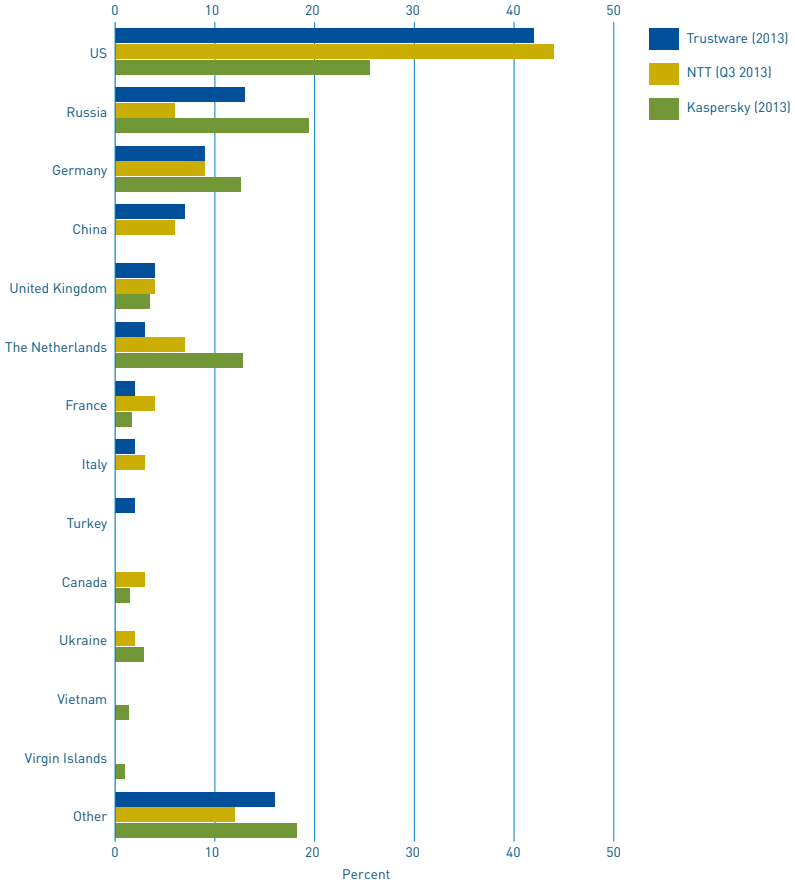


FIGURE 19 MALWARE HOSTING PER COUNTRY IN 2013 (NTT, 2014; TRUSTWAVE, 2014; KASPERSKY, 2014)

Some trends affecting tools and techniques
The reports we investigated point to several ongoing trends that have changed the tools and techniques used by perpetrators.

Mobile devices are next. Attack services and exploit kits aimed at mobile platforms are proliferating, a trend that is set to continue in coming years.[18] Because ever more people migrate from traditional PC-like platforms to mobile devices, this creates a new operating environment for perpetrators. The increased use of mobile devices also creates new opportunities for identity breaches and theft of personal sensitive data.[19]

The Cloud is on the horizon and moving fast. The trend in the adoption of cloud computing is expected to increase. In 2015 cloud computing is expected to account for nearly 34% of traffic at the world's data centers – the huge computing stations that now process and distribute most of the Internet's information.[20] Thus, data farmers and the service providers using and managing these data centers will become the focus of perpetrators' attention.

Internet of Things. Attacks on interconnected devices as part of the Internet of Things (IoT) move from proof-of-concept to mainstream risks. Altogether manufacturers of Internet of Things devices (mostly for consumers) have failed to implement basic security standards, creating an easy opportunity for hackers, while users are often unaware of the vulnerabilities an IoT device creates.[21] The impact on the individual consumer might be limited now, but society as a whole will need to start dealing with the negative consequences of making their 'dumb' devices 'smart'.

Ransomware. A specific malware called Ransomware has already claimed many victims in the last two years. This malware entirely locks your computer or device and will only reverse it in exchange for payment. More recently, this has evolved into nastier cryptoware, used to take all personal data hostage (while making the same demand for ransom). It is expected to evolve into mobile cryptoware soon. One report indicates ransomware attacks have grown 500% since 2013.[22]

2.5 Targets

2.5.1 Location of targets

Attacks are not evenly dispersed across the globe. As we have seen in section 2.3.2, some countries are more prolific than others in hosting cyber attacks. Similarly, some countries host more attractive targets to be attacked. It should be noted that the results in the figure below may be skewed because of the many number of US data attacks that the reports rely on. It may well be that the US and the UK host many of the victims in cyber space, but a more precise assessment would be needed for specific types of attacks (e.g., espionage, cyber crime) to create a more insightful picture.

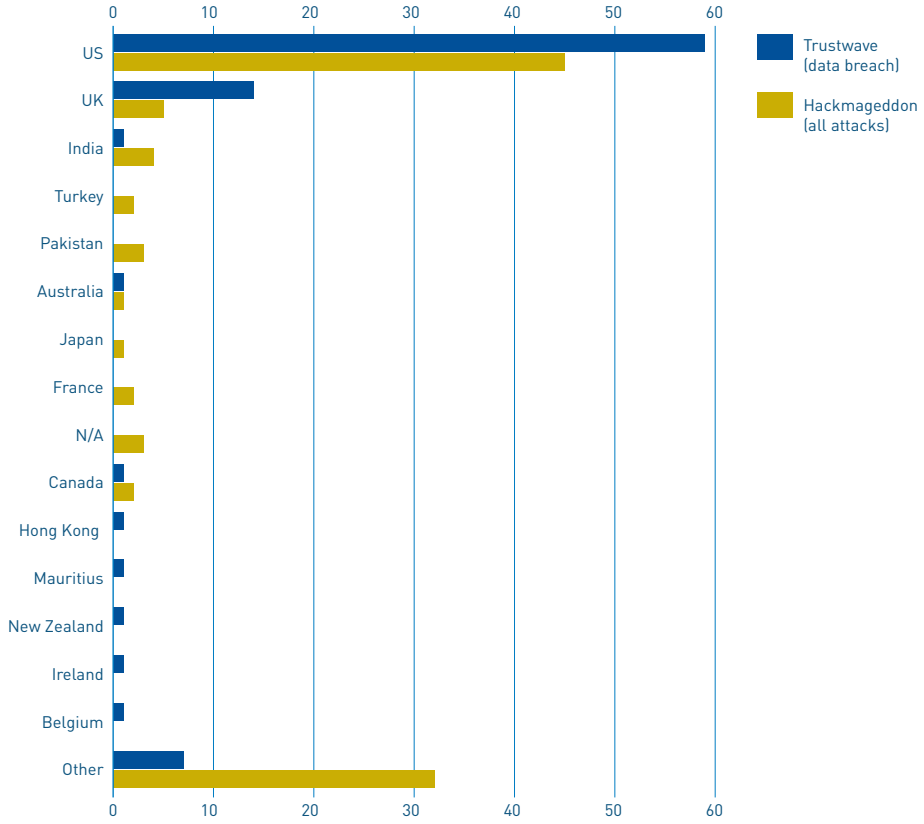


FIGURE 20 SHARE OF TOTAL ATTACKS ON TARGETS IN EACH COUNTRY IN 2013, ACCORDING TO HACKMAGEDDON.ORG (2014) AND TRUSTWAVE (2014)

Only a few other reports provide an assessment of attacks per country – and most are rather vague. One report notes that almost half of all attacks use IP addresses in the US.[23] It also provides a map showing number of incidents, but it does not provide the raw scores, nor any further explanation of the color coding. The report notes that about half of all attacks were aimed at US actors. But apart from that, it shows considerable differences with the Hackmageddon.org and Trustwave reports. Note that the UK is classified as experiencing few attacks, while Sweden is singled out as a country experiencing a high number of attacks.

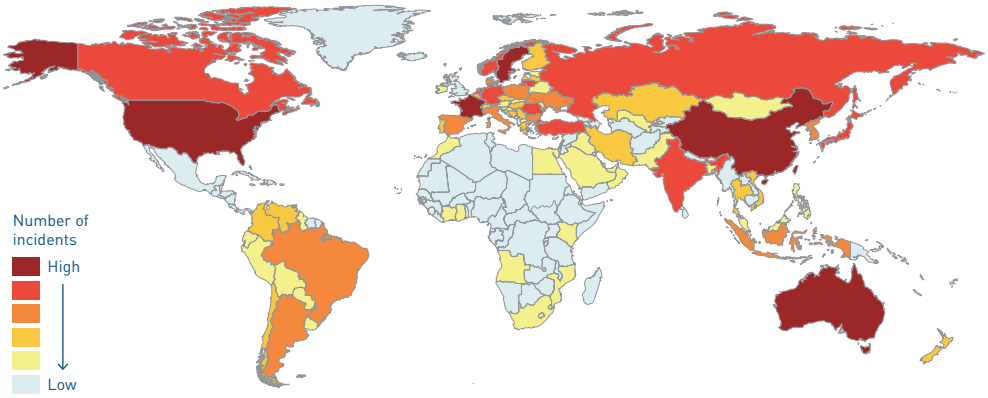


FIGURE 21 MAP SHOWING CYBER INCIDENTS PER COUNTRY ACCORDING TO NTT IN 2013. HIGHEST RANKED COUNTRIES ARE AUSTRALIA, US, FRANCE, SWEDEN, CHINA. THESE ARE FOLLOWED BY CANADA, INDIA, RUSSIA, NORWAY, GERMANY, THE NETHERLANDS, TURKEY, UKRAINE, MYANMAR, JAPAN, AND ESTONIA. (NTT, 2014)

2.5.2 Sectors under attack

Of all sectors, the government and the financial services stand out as main targets (see Figure 22). The five reports that investigate attacks per sector differ substantially in the classification of sectors and their assessments of the attacks conducted.

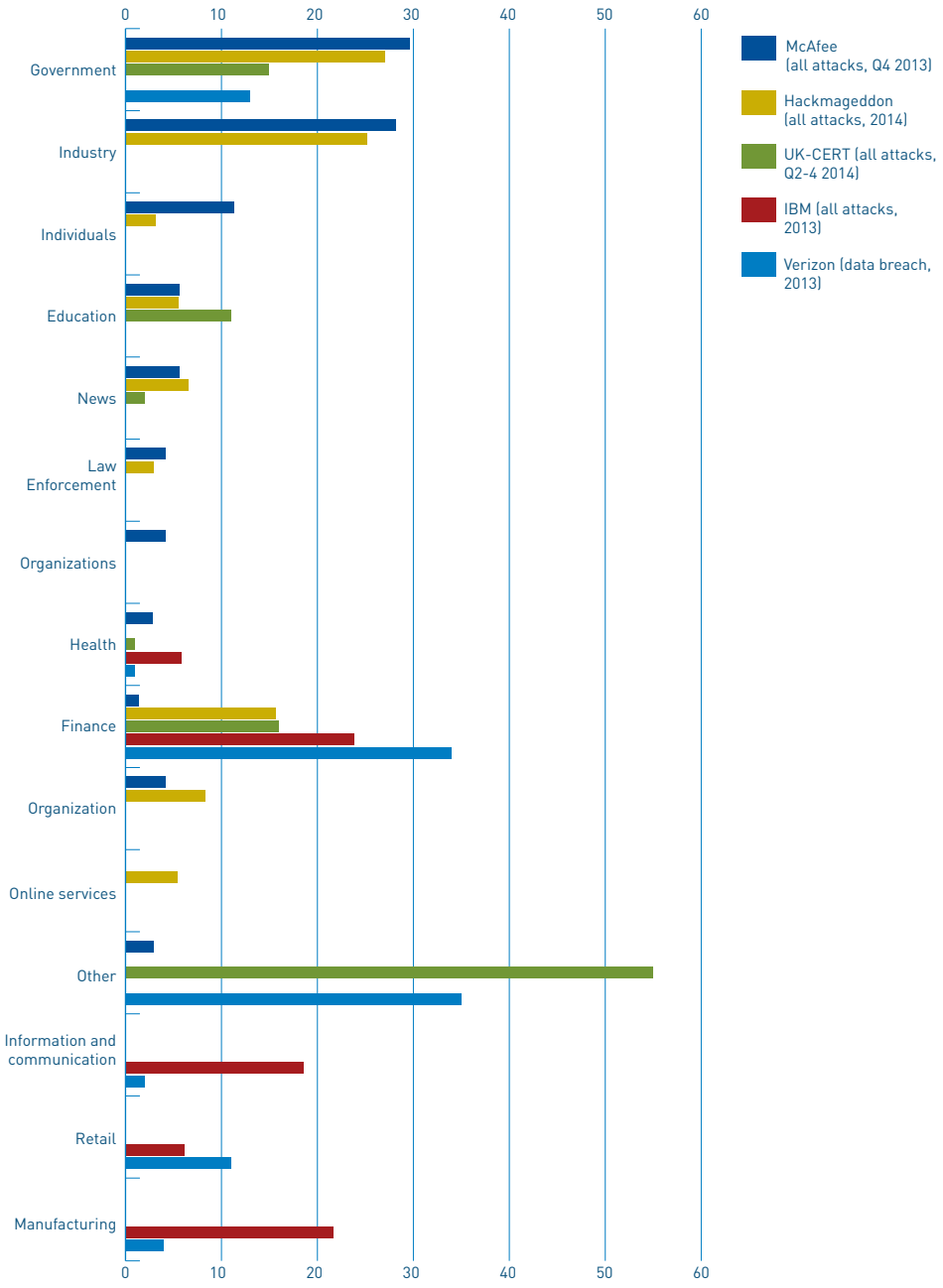


FIGURE 22 CYBER ATTACKS PER SECTOR IN 2013 (VERIZON, 2014; IBM, 2014; HACKMAGEDDON.ORG, 2014; MCAFEE, 2013) AND 2014 (UK-CERT, 2014)

Vulnerability of critical infrastructures

Some reports we looked at suggest that the security of industrial control systems (ICS) and Supervisory Control And Data Acquisition (ICS/SCADA) systems that manage most critical infrastructures, will deteriorate. ICS/SCADA systems are often out-of-date, typically 10 years or more behind the mainstream desktop environment in terms of security.[24] In addition, the cooperation between governmental bodies and private organizations (who operate the majority of the critical infrastructure) is often poor.[25]

2.6 Impact

Cyber attacks can have various negative effects on organizations – both directly and indirectly. They can lead to financial loss, but can also damage reputation or lead to a loss in customers (see Figure 23).

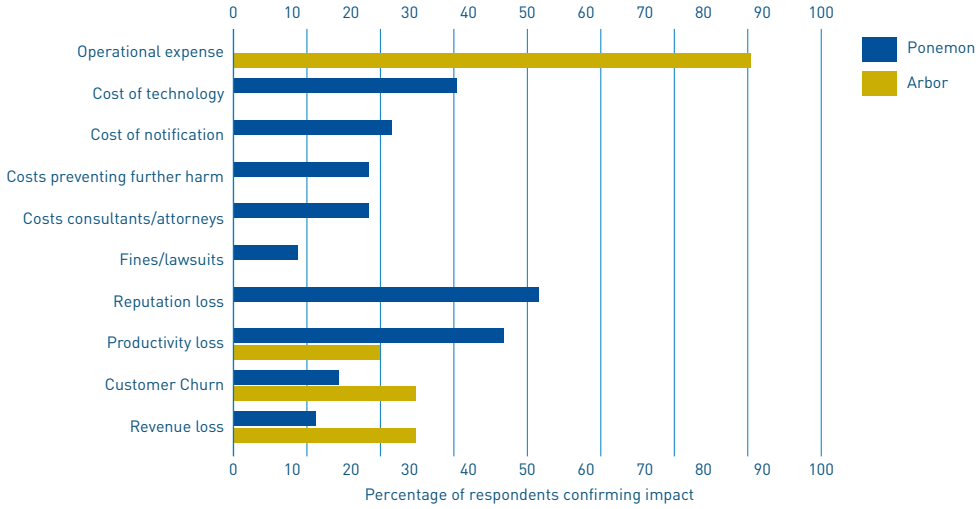


FIGURE 23 DIFFERENT TYPES OF NEGATIVE IMPACT RESULTING FROM CYBER ATTACKS IN 2013. THE ARBOR REPORT FOCUSES ON DDOS ATTACKS.

Damages are often difficult to put into hard figures, because companies may be reluctant to report on attacks and the losses theys led to, and because losses can be indirect (e.g., customer chum) or spread out over a longer period of time (e.g., through reputation loss). Three reports attempt to gauge the average financial impact of cyber attacks on organizations (see Figure 24). Indications are for sizable companies of over 500 employees (Ponemon) or a turnover of multiple millions (PWC).

REGION/COUNTRY	PWC	KASPERSKY	PONEMON
NORTH AMERICA	2,9		
US		0,433	12,97
EUROPE	1,3		
France		1,31	6,38
Germany		0,471	8,13
Italy		0,675	
Turkey		0,668	
UK		1,66	5,93
Spain		0,631	
Russia		0,472	3,33
ASIA PACIFIC	2,3		
China		1,06	
Japan		0,448	
Australia		0,588	3,99
India		0,86	
SOUTH AMERICA	2		
Brazil		1,8	
Mexico		0,411	

FIGURE 24 AVERAGE ESTIMATED FINANCIAL LOSSES (IN MILLION USD) FOR SIZABLE COMPANIES IN SELECTED COUNTRIES IN 2014 (PWC, 2014; KASPERSKY 2014; PONEMON 2014)

The study by Ponemon, which surveyed 257 companies from all over the world with over 500 employees, distinguishes per company size, and suggests that costs increase incrementally with company size. To put this into perspective: this amounts to around 437 USD per employee for the smallest quartile of the sample, ranging up to 1,601 USD for the largest quartile.

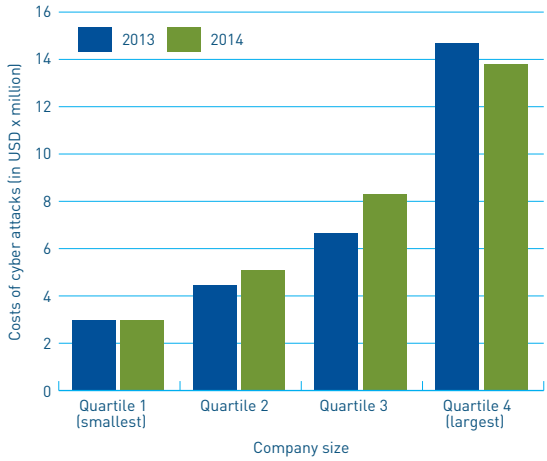


FIGURE 25 COSTS OF CYBER ATTACKS PER SIZE OF COMPANY IN 2013 AND 2014 PER QUARTILE OF SAMPLE OF 257 COMPANIES WITH OVER 500 EMPLOYEES (PONEMON, 2014)

PWC gives a similar assessment. In 2014, companies with revenues below USD 100m suffered $0.41m in losses; companies with revenues between USD 100m-1bn suffered $1.3m in losses; while companies with a turnover of over USD 1bn suffered almost $6m dollars in losses (see Figure 26).

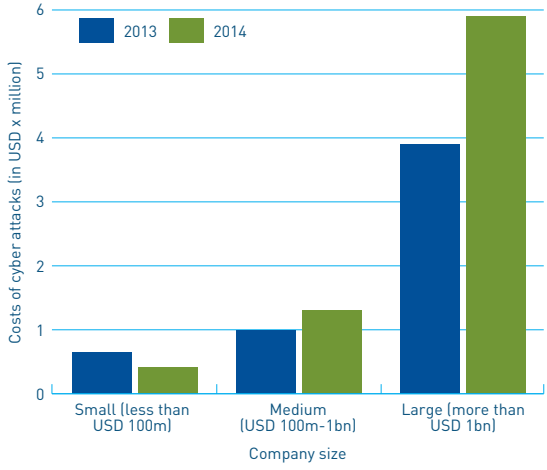


FIGURE 26 COSTS OF CYBER ATTACKS PER SIZE OF COMPANY IN 2013 AND 2014 ACCORDING TO PWC, BASED ON A SURVEY OF OVER 9,700 SECURITY, IT, AND BUSINESS EXECUTIVES AROUND THE WORLD (PWC, 2014)

A McAfee report estimates that global cyber activity adds up on the national level and costs around 0.8% per GDP annually. It provides an assessment of the total GDP lost for several countries worldwide (see Figure 27). Unsurprisingly, the impact is particularly large in richer countries. Notably Germany and the Netherlands report high GDP losses, although the report notes a "difference in the methodologies used to calculate cost, along with difficulties in acquiring information from companies on losses".[26]

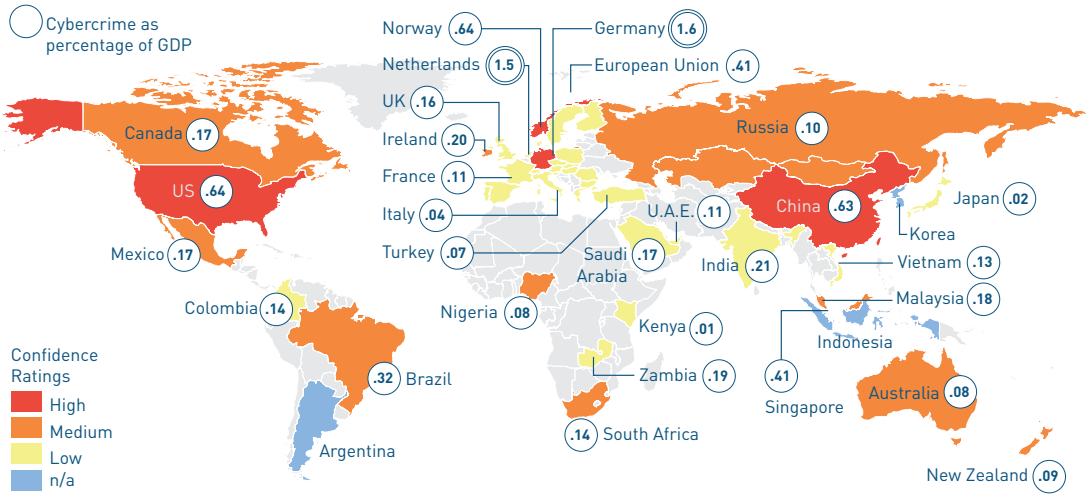


FIGURE 27 ESTIMATED COSTS OF CYBER CRIME AS A PERCENTAGE OF GDP (MCAFEE, 2015)

2.6.1 Impactful cyber attacks in 2014

What were the most prominent cyber attacks in 2014? This final paragraph provides an overview of some of the most damaging cyber attacks in the previous year.

ORGANIZATION ATTACKED	TYPE OF INDUSTRY	REGION	DATE EXPOSED	DIRECT FINANCIAL LOSS (USD) / DATA LOSS
Target	Retail	United States	1-1-2014	USD 148,000,000
JP Morgan Chase	Finance	United States	7/1/2014	83 million accounts
Multiple (Carbanak cyber attack)	Finance	Around 30 countries	16-2-2014	USD 1,000,000,000
Korea Credit Bureau	Finance	South Korea	March 2014	Personal financial information from 105,8 million banking accounts
Yahoo	Communication	United States	1/3/2014	USD 273 million users affected
eBay	Retail	United States	April 2014	233 million buyers affected
Multiple (Heartbleed attack)	Various	Various	April 2014	N/A
Boleto Bancaria - Boleto	Finance	Brazil	2-7-2014	USD 3,750,000,000
Home Depot	Retail	United States	9-8-2014	USD 62,000,000
Sony Pictures	Entertainment	United States	11/24/2014	USD 15,000,000

TABLE 1 OVERVIEW OF IMPACTFUL CYBER ATTACKS IN 2014

1. **Target:** In early January 2014, Target – a US based retail company – was the victim of a massive data breach. Personal records of more than 70 million shoppers and more than 40 million credit card details were stolen as a result. The attack reportedly cost Target USD 148 million, and resulted in a 46 percent drop in profit and 14 percent drop in the stock market. Additionally, Target spent an additional USD 61 million in anti-cyber attacks technology as a result.[27]

2. **Carbanak cyber attack:** Since 2013, a criminal gang with members from Russia, Ukraine, China and parts of Europe used targeted attacks to steal up to USD 1 billion from financial institutions in as many as 30 countries.[28]

3. **JP Morgan Chase:** In January 2014, over 83 million accounts at the investment bank JP Morgan Chase were hacked.[29] The breach is one of the biggest in history.

4. **Korea Credit Bureau:** In March 2014, over 100 million credit card and account details were stolen from the Korea Credit Bureau. Estimates point to up to 20

million affected citizens. The attack was instigated by an employee, who stole the data in 2012.[30]

5. **Yahoo:** At the beginning of March 2014, the Yahoo saw a hack that left personal data from 273 million users of its mail service compromised.

6. **eBay:** Over 230 million users' data from eBay was stolen between February and March 2014. Later, the Syrian Electronic Army claimed responsibility for the attack, framing it as hacktivism, and stated that they "didn't do it to hack people's accounts".[31]

7. **Heartbleed:** In April 2014, a vulnerability was detected by Google and Finnish security firm Codenomicon. The security flaw remained undisclosed for two years, and allowed attackers to misuse OpenSSL software, used in many web servers. Attackers were able to steal data unnoticed (e.g., passwords and credit card data) unnoticed.

8. **Boleto Bancario:** In July 2014, a report by RSA Research group unveiled a malware that compromised over 400,000 Boletos transactions over a period of two years. According to the report, the expected amount of money stolen based on the transactions is estimated to be close to USD 3.7 billion, however it is unclear whether the perpetrators successfully siphoned the money.[32]

9. **Home Depot:** In September 2014, Home Depot suffered a major data theft that comprised approximately 40 million credit and debit cards. Home Depot was reportedly expected to pay approximately USD 60 million to cover the cost of the attack, including legal fees and overtime fees for staff.[33]

10. **Sony Pictures:** In November 2014, Sony Pictures was hit by a cyber attack. According to the US government, the attack was launched from North Korea, but this allegation is widely disputed. The investigation and the remediation cost amounted to USD 15 million.[34]

3 TECHNOLOGY TRENDS IN A SOCIETAL PERSPECTIVE

3 TECHNOLOGY TRENDS IN A SOCIETAL PERSPECTIVE

3.1 Introduction

The previous chapter listed a multitude of important current and evolving cyber security trends. These trends have been analyzed by comparing the reviewed documents and extracting similar or matching trends information. However, many of the selected reports use a technology-centric approach to describe the threats. Most of the cyber security vendor reports base their analysis on the information they gathered from their own infrastructure and their customers. In addition, every reporting organization describes the threats and trends from their own perspective, scope, and reference datasets. This creates a bias when extrapolating trends and threats from their 'limited' dataset and explains the technology-centric focus on the issues at hand.

This chapter is focused on getting a better understanding of the direction in which these threats and trends seem to develop. In this, we did not aim for a comprehensive coverage of all cyber threats and trends. Instead, we highlight some trends that are emerging and noted in these documents that we deem particularly noteworthy. The analysis is based on a quick scan of the corpus of cyber threat reports and considers the societal drivers and technology trends that affect the cyber threat environment. By highlighting some emerging trends, it aims to expand our view beyond the current threat landscape. As in chapter 2, the sections below focus on perpetrators, targets, and tools and techniques.[35]

3.2 Perpetrators

This section highlights how three societal and technological developments affect various groups of perpetrators.

3.2.1 A new exploit-trade economy on the rise

Information about software vulnerabilities as an entry point for exploitation can be very profitable for the right 'customer'. There is a large and visible emerging trend in this area, creating a whole new economy where well-intended ('ethical') 'white-hackers', malicious, 'black-hat' hackers and other cyber experts professionalize their activities to sell vulnerabilities found in an ICT infrastructure or in software ('zero-days').[36] According to cyber security guru Bruce Schneier, the zero-day exploit market has grown from almost non-existent to full maturity.[37] The danger of this new economy is that it provides security for the 1% who can afford it; for others, vulnerabilities remain secret, unpatched, and open to be exploited.

This means the role and power of hackers will increase. When security vulnerabilities are disclosed in a responsible way (hence 'responsible disclosure'), it provides an incentive to the software vendor or those responsible for the specific infrastructure, product, or service to patch the vulnerability. In the end, this approach improves the security of society as a whole. However, ultimately the hacker decides how and to whom he or she will disclose newly discovered vulnerabilities.

3.2.2 State actors and OCGs converge capabilities

A convergence of tools and techniques is increasingly taking place between Organized Crime Groups (OCGs) and state actors.[38] A Mandiant report describes state actors[39] using tools widely deployed by cyber criminals. As the tactics used by these actors merge, discerning their goals and identifying the actual perpetrators becomes even more difficult. This also impacts the risk mitigation process of target organizations, because it becomes less clear where the threat comes from and for what reason the organization is targeted.

State actors sometimes lack the cyber capabilities to successfully execute an attack themselves, it is not an unlikely scenario that they will increasingly hire OCGs and 'cyber mercenaries' to become part of their approach to achieve the state actors' goal (see also section 3.2.3 and 3.4.2). In addition, this allows states to obfuscate or hide their involvement in attacks.

3.2.3 Cyber space as a new domain of warfare

Because states are rapidly developing offensive cyber capabilities, the threat of cyber weapons becoming a central ingredient in warfare is increasing. States have used digital means in warfare for some time now. But increasingly, states are also recognizing cyberspace as a new warfare domain. Governments are developing

strategies and military doctrines to integrate new cyber capabilities into the existing military apparatus, with cyberspace a domain to be used for intelligence gathering and defensive and offensive purposes. However, little is known about the maturity of those capabilities. For example, while all nations developing cyber capabilities mention defensive and intelligence purposes, only a few openly talk about offensive ambitions (the U.S. and The Netherlands are amongst those few).[40]

There is much discussion about the limits of cyber warfare. Although attribution remains a bottleneck for providing solid evidence of state-involvement, there are ample examples of cases where states were likely involved in large scale cyber attacks – from Stuxnet, to the three week wave of cyber attacks in 2007 against Estonia. It is likely that efforts continue to achieve new cyber warfare capabilities. This opens up a new field of uncertainties: will we see an arms race in cyber space, a spur for so-called 'cyber soldiers' and 'cyber weapons'? And how will this change the face of warfare?

3.3 Targets

This section considers the various types of groups or assets that will get increasingly targeted by perpetrators. It highlights four trends at different levels.

3.3.1 Individuals and personal information: ID theft 2.0

Identity theft is set to evolve as a new trade on the 'dark markets'. ID-theft is often caused by data breaches somewhere in the supply chain of other organizations.[41] The trend is for perpetrators to focus more on 'who you are' than 'what you have': with a stolen identity, a perpetrator has multiple vectors of approach and opportunities to seize. Both governments and private organizations are increasingly stimulating their citizens and customers to take the next step in electronic identification. The flip side of this is that all this digital information will make them an even more interesting target for perpetrators.

3.3.2 Big Data herders and trust providers become a focal point for attacks

More companies will develop business cases around big data and act as data brokers by amassing large amounts of data. Given the potential value and multipurpose use of this data, it is also expected that more targeted attacks on data brokers occur, mainly for economic reasons but also for politically motivated attacks.[42]

The impact of cyber threats regarding big data is multi-level; at storage level (attacking the actual databases), at transformation level (gaining access to collected data even before anonymization if / when applicable) and at analysis level (gaining unlawful

access to information that can, for instance, render solution vendors more competitive).[43]

From an organizational point of view, third parties like cloud providers, trust providers and managed service providers can become the center of attention or at least the stepping stone to attack a certain target further in a supply chain. One example is the 2011 RSA spear-phish attack, which is seen as a stepping stone to further attacks on defense contractors such as Lockheed Martin, L-3 and Northrop Grumman.[44] Trust and Service providers could well become a key vulnerability in an organization's supply chains, as cybercriminals and other perpetrators target them rather than the organizations directly.[45]

3.3.3 GPS and its widespread services for PNT

Although security in technology improves step-by-step, some domains are still waiting to be targeted. Critical infrastructure sectors and systems are relying on space-based Global Positioning Satellites (GPS) for positioning, navigation, and timing (PNT). But while the GPS system is considered to be highly accurate, very robust and reliable, its PNT signals are vulnerable to disruptions due to naturally occurring phenomenon such as space weather events or malicious interference. Widespread reliance on space-based GPS for positioning, navigation, and timing services presents a cyber security risk that has not been mitigated to a thorough extent yet.[46] Although this might not be of direct interest to a cyber criminal, nation states will be interested in this vulnerability, as it increases the effectiveness of their cyber capabilities.

3.3.4 Internet of Things (IoT) and the cascade of effects

The potential impact of cyber attacks is becoming more severe due to increasing levels of digitization and the interdependencies that are created by it.[47] However, many cyber security professionals still approach internet security similar to how financial experts acted prior to the 2008 financial crisis: by assuming that the risk posed to the system is merely a sum of all individual risks, and ignoring cascading effects.[48] Combined with the poor patching strategy of many organizations this will likely lead to a large negative impact of cyber attacks.[49]

The impact of the increasing levels of interdependencies caused by digitized systems within society is an eco-system that has grown so large in complexity, that the risks involved are hard to assess. This makes it even harder to determine and implement the appropriate mitigation measures. In addition, the increased interdependencies has also created a complex and intertwined eco-system of responsibilities for the digitized products and services.

This digitization is largely fueled by innovation in general. Although innovation is generally considered as good and a driver for the growth of Western economies, at the same time it creates new tools and techniques for perpetrators to attack targets. A selection is explained further in the next section, but two examples can be given, both related to the increased use of ICT in healthcare. The first is a misuse of ID-related and personally sensitive information as a result of data breaches.[50] The second one involves the use of implants and other medical devices that contain ICT to inflict personal harm. Linking these medical devices to a network and tampering with its capabilities can cause potentially fatal harm to individuals. Examples of devices such as pacemakers and insulin pumps being vulnerable to cyber attacks are already known.[51]

3.4 Tools and techniques

The current section deals with tools and techniques having direct relevance to cyber security not covered in earlier sections. It presents the difficulties to identify perpetrators and their motivations, to apply defence mechanisms against the ever increasing computing power, and the way that cyber criminals deploy techniques and business models to stay ahead.

3.4.1 Anonymization as a supporting trend

The anonymization techniques like The Onion Router (TOR) services used in parts of the Internet that are known as Darknets, allow users to communicate freely without the risk of being traced. On the one hand these are legitimate tools for citizens to protect their privacy or for certain groups repressed by dictatorial or authoritarian regimes to interact with the rest of the world. However, the features of these privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit online trade in drugs, weapons, stolen goods, forged IDs and sexual exploitation of children.[52]

The TOR project estimates that about 30,000 unique hidden services on the TOR network make up around 3.4% of the total traffic on the entire network. Also the TOR search engine Onion City has indexed about 350,000 TOR hidden pages.[53]

As a Europol study suggests, several large marketplace services exist (and continuously change in name, form and content). In many of these marketplaces, digital currencies are used to exchange the illicit goods and services, as many of the digital currencies also provide the user anonymity. Because it is very hard to get a clear picture of the sheer size of the Darknets, we can only assume that this anonymization trend supports the perpetrators in the advancement of their tools and techniques.

3.4.2 Cyber attacks out in the open but camouflaged

It is expected that perpetrators will use their creativity to combine cyber attacks as part of larger cyber operations, where the malicious cyber attacks will only be a means to gain (an unfair) advantage in legitimate acts. As the end result is a legitimate monetary gain, inside knowledge of a large merger and acquisition activity or otherwise, the cyber attack behind it is even harder to detect. It also becomes more difficult to analyze the attacks' true purposes, thus giving the perpetrator an advantage. An example is given below.

Stock market manipulation

Stock market manipulation is a growth area for cybercrime. By breaking into a company's networks or into the networks of its lawyers or accountants (which can sometimes be an easier target), cybercriminals can acquire inside information on acquisition and merger plans, quarterly revenue reports, or other data that could affect a company's stock prices. Criminals taking advantage of this information for trading could be hard to detect, as it might look like a normal trade, especially if it was carried out in another stock market. Using chat rooms and social media for "pump and dump" is a well-established technique, with criminals providing false information about a company's prospects and then cashing in when the market reacts. Turkey's financial regulators, for example, found suspicious activity intended to manipulate markets and stock prices that went beyond "pump and dump" schemes. For high-end cybercriminals, cybercrime may be morphing into financial manipulation that will be exceptionally difficult to detect [Center for Strategic and International Studies/ McAfee - The economic impact of cybercrime and cyber espionage, 2013].

3.4.3 Encryption failure leads to trust erosion

Encryption is the default approach to secure Internet interaction. However, some advocate that encryption will fail to deliver its promise due to vastly improved computing power combined with backdoors in software. This will lead to trust erosion in the Internet and E-services. New encryption techniques will evolve, but it will take time for users and supporting technology to catch up.[54]

As good encryption is a backbone of secure communication, the impact of the lack of new trustworthy and viable encryption system-alternatives for society is very high. In addition, encryption as a concept is hard to understand for the average Internet user.

Perpetrators are aware of this and thus will create new and creative modi operandi to exploit this fact, which may result in even more trust erosion in the Internet and E-services.

3.4.4 Big bad data analytics

Data analytic techniques are nowadays used to analyze big data, and are already being used extensively by commercial organizations and governments. We also identified a trend in the adoption of big data analytics techniques for criminal purposes. The same analytics approach used by businesses, police and intelligence services, can be copied by a perpetrator. For instance, social networking analysis can be used to select the persons of interest in an organization who can be most efficiently targeted by spear-phishing. This approach will create all sorts of new opportunities for cyber criminals, such as extraction of data of interest, and ID information enhancement.[55]

3.4.5 IT is becoming a business CaaS for criminals

As mentioned in the previous paragraph, perpetrators continue to increase their illegal trade and commercialize products and services. The creativity of the perpetrators knows few boundaries. Their activities can be summarized as a service of tools, programs, botnets, denial-of-service attacks, malware development, data theft and password cracking for those (criminals) who neither possess the knowledge to execute the cybercrime themselves, nor have the resources to support their own criminal activities.[56] The Cybercrime-as-a-Service (CaaS) business model provides a wide range of criminal services that facilitate almost any type of cybercrime on a commercial basis. The financial gain that hackers receive from offering these services stimulates the commercialization of cybercrime as well as its innovation and further sophistication.[57] The CaaS trend also lowers the threshold for all who seek to buy or hire an attack to support their own malicious purposes, including the nation states as mentioned in paragraph 3.2.2.

4 RESPONSE TO CYBER THREATS

4 RESPONSE TO CYBER THREATS

As the previous chapters make clear, cyber threats are becoming more numerous, more sophisticated and more impactful. At the same time, our dependence on the seamless functioning of cyber infrastructure and the services it provides is steadily increasing.

These trends demonstrate that security of cyberspace is essential for nations' economic development and national security. And indeed, many countries take cyber threats very seriously. This, in particular, applies to those countries that have moved ahead in adopting ICT and as a result are more vulnerable to failures in cyber security. One indicator of the importance attached to cyber threats by governments is the development of a cyber security strategy. This chapter starts by summarizing information on national cyber security strategies based on published articles and reports.

This chapter also reviews other metrics that should be helpful in gauging cyber security efforts that have been (and are being) undertaken by various actors including private sector companies and individuals. One indicator of such efforts is the amount of money spent on cyber security. Finally, this chapter looks at several indices of cyber security (and related concepts). These indices try to summarize various pieces of information sources into an overall assessment of national cyber security.

4.1 National cyber security strategies

National cyber security strategies (NCSS) are a new phenomenon: the first strategies started to appear only in the first years of the 21st century. The United States was one of the first countries to publish such a strategy in 2003.[58] Clearly demonstrating that cyber security has already become a national priority.

Although NCSS is a very recent development, the website of the European Network and Information Security Agency (ENISA) currently lists 33 countries from around the world with an approved NCSS, and another 8 where an NCSS is under preparation.[59]

In the European Union 25 member states have an NCSS (either completed or under preparation). International Telecommunication Union (ITU) and ENISA have published manuals on developing a national cyber security strategy. Our goal in this section is to provide a brief overview of major concepts and issues within NCSS based on several published articles and reports.

4.1.1 Definitions and scope

Interestingly, among 18 NCSS analyzed in an article by Eric Luiijf and others (2013) only 8 explicitly define the notion of cyber security.[60] Even when cyber security is defined there are often visible differences in the definitions used . Some include both intentional and non-intentional threats while others focus exclusively on deliberate attacks (Canada, for example).[61] The UK's strategy expands threats to cyberspace to include physical and electromagnetic disruptions. Another differentiation in defining the scope of cyber security is whether it includes only systems and devices connected to the Internet or, a broader range of systems and devices, including chip cards, IT systems embedded in various devices, and industrial control systems.

In recent years the scope of practically all cyber security strategies has expanded from protecting individuals and organizations to protecting society as a whole, which is a result of increasing reliance of all aspects of our life on ICT.[62] Practically all NCSS emphasize the adoption of an integrated and comprehensive approach and the importance of public-private cooperation in addressing cyber security threats. Many cyber security incidents clearly demonstrate that without end-users adopting basic computer security hygiene rules they will continue to be highly vulnerable to future cyber attacks. Given the global nature of the Internet, the international dimension of national cyber security and enhanced international cooperation is one of the priorities in many NCSS. Agreeing on the internationally accepted rules of behavior in cyberspace might be difficult, however, even between close allies.

Tensions between promoting the economic benefits of the digital economy and protecting IT systems are present in all countries: they are about finding the optimal balance between investment in cyber security (which is costly) and realizing full economic benefits of progress in ICT. Countries put different weights on economic aspects of cyber security. Some countries, including the UK, see improved cyber security as a way to develop a competitive advantage for the country in cyber space. Others, including Germany and Spain, emphasize "the need to maintain or develop technological independence or sovereignty in core strategic IT competences."[63]

4.1.2 Risk perception: threats, actors

An important part of cyber security strategies is the characterization of cyber threats that a nation is facing. The perception of cyber security risks have often been driven by significant accidents, such as denial of service attacks against Estonia in 2007 and China's digital espionage activity.[64] Practically all countries with an NCSS consider cyber threats as one of the top national security issues in overall national risk assessment. At the same time, a recent RAND report notes that "higher prioritization of cyber threat has not consistently translated into greater resource allocated to the area".[65]

There is a broad consensus in NCSS that the most important risk dimensions of cyber threats are toward economic prosperity and critical infrastructure. All 18 countries analyzed by Luiijf et. al. (2013) list these two dimensions in their NCSS, at least implicitly (see Table 2). National security aspects of cyber threats were emphasized less often, but were still the third most frequently mentioned type of risk in NCSS. Other dimensions of cyber threats find less agreement in NCSS. Some strategies include such dimensions of cyber threats as undermining public confidence in the use of ICT, negative impact on social life or defense capabilities. Others omit them all together. We can speculate that some countries might consider these second-order effects or see them as part of a broader dimension. In the case of cyber threats to defense capabilities, they might purposely exclude this topic from NCSS and address it elsewhere (e.g., the US).

With respect to threat actors there is a broad agreement between various NCSS. All strategies mention (explicitly or implicitly) individual criminals and organized criminal groups as important threat actors. Cyber threats from foreign states is mentioned in 13 strategies. The same number of NCSS mention terrorist groups as a significant (potential) source of cyber attacks. According to available empirical data, terrorist groups have not been behind many cyber attacks so far. At the same time, use of the Internet for fundraising, recruitment, propaganda and other goals is often crucial for such groups. Hacktivists (groups such as Anonymous and LulzSec) have received much less attention in cyber security strategies but were behind some of the most publicized cyber attacks. Two nations, Germany and Japan, identify as a potential threat not a specific actor, but a structural mismatch between ICT development and an appropriate level of cyber security.[66] Some researchers note that in the last few years "the emphasis has changed from a focus on transnational, terrorist threat actors to a framing of cyber security in terms of defense and increasingly offensive capabilities against cyber criminals, state actors and their proxies."[67]

Finally, one consideration that emerges from the analysis of the existing strategies as well as from OECD consultation with non-governmental stakeholders is that cyber security policy should be much more evidence-based and rely more on data and indicators rather than subjective perceptions.[68]

	CYBER THREATS TO:						
COUNTRY	CRITICAL INFRASTRUCTURE	DEFENSE CAPABILITIES	ECONOMIC PROSPERITY	GLOBALIZATION	NATIONAL SECURITY	PUBLIC CONFIDENCE IN ICT	SOCIAL LIFE
AUS	●	●	●		●		●
CAN	●	●	●		●		●
CZE	●		●		●		○
DEU	●		●	●	○		
ESP	●		●		●	○	
EST	●		●		○		●
FRA	●	○	●		●		
GBR	●		●		●	●	●
IND	●		●	○			
JPN	○		●	●	●		●
LTU	●		○		○	●	
LUX	●		●			○	
NLD	●	○	●		○	●	●
NZL	●		●		●	○	
ROU	●	●	○		●		
UGA	●		●			●	
USA	○		●		●	●	
ZAF	●		●		○	●	
Count	18	5	18	3	15	9	7

NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

TABLE 2. CYBER THREATS IN NCSS
SOURCE: LUIIJF, E., K. BESSELING, AND P. DE GRAAF.

	CYBER THREATS FROM:						
COUNTRY	ACTIVISM/ EXTREMISTS	CRIMINALS/ ORGANIZED CRIME	ESPIONAGE	FOREIGN NATIONS/ CYBER WAR	TERRORISTS	LARGE-SCALE ATTACKS	MISMATCH OF TECHNOLOGY AND SECURITY
AUS		●	●		●		
CAN		●	●	●	●	○	
CZE		●		●	●		
DEU		●	●	●	●	●	●
ESP	○	●	●	●	●	○	
EST		●		●	●		
FRA		●	●	●	●		
GBR	●	●	●	●	●	●	
IND		●		●		○	
JPN		○	○	●		●	●
LTU		●				●	
LUX		●					
NLD	●	●	●	●	●		
NZL	●	●	●		●		
ROU	●	●	●	●	●		
UGA		●		●	●	○	
USA		○	●	●	●	○	
ZAF		●					
Count	5	18	11	13	13	9	2

NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

TABLE 3. CYBER THREAT ACTORS IN NCSS

SOURCE: LUIIJF, E., K. BESSELING, AND P. DE GRAAF.

4.2 Responses by EU firms and citizens

A national cyber security strategy is a high-level approach demonstrating the attention to cyber security issues on the part of national governments. Still, the overall level of national cyber security is largely determined by the actions of millions of organizations and individual users of ICT. In this section we will briefly review existing data on cyber security awareness and preparedness of the EU organizations and citizens.[69]

4.2.1 Size matters

One way to judge the cyber security preparedness of an individual enterprise is to see whether it has a formally defined cyber security policy[70], which can be viewed as an analogue of an NCSS at an enterprise level. A Eurostat survey shows that an answer to this question strongly depends on a company's size: 65% of large enterprises (defined as having more than 250 employees) had such a policy, while this percentage drops to 43% for medium enterprises (between 50 and 250 employees) and further to 22% for small enterprises (less than 50 employees).[71] The share of enterprises having a formally defined ICT security policy also varies significantly between different countries and economic sectors. The highest percentages were recorded in northern European countries – Sweden, Norway and Denmark, where such percentages were above 40% of all enterprises. In contrast, in lagging EU member states this percentage was below 10% (see Figure 28).

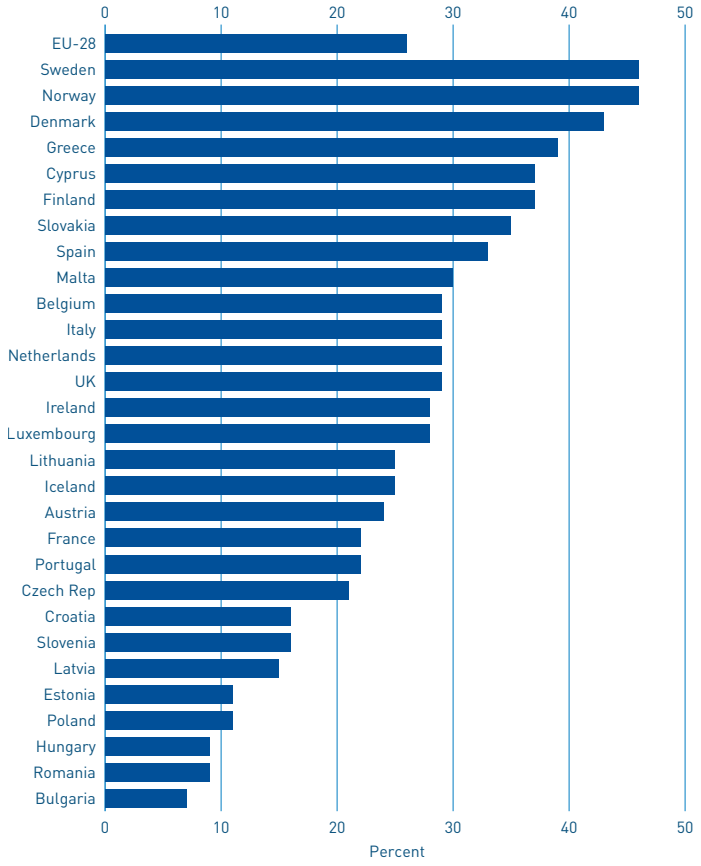


FIGURE 28 PERCENTAGE OF EU COMPANIES HAVING A FORMALLY DEFINED ICT SECURITY POLICY BY MEMBER STATE, % OF ALL ENTERPRISES (WITH 10 AND MORE EMPLOYEES). SOURCE: EUROSTAT, 2010 (DATA CODE: ISOC_CISCE_RA)

4.2.2 Sectoral awareness

In terms of economic sectors, by far the highest level of cyber security awareness was observed in the financial sector. Almost 80% of all financial institutions had an ICT security policy. This is related to the fact that financial institutions are some of the most lucrative targets for cyber criminals and their exposure and potential losses to cyber threats are very high. High level of cyber risk and heavy regulation of the sector has pushed its efforts to improve its preparedness. In such less technically sophisticated sectors such as construction, hospitality and transportation, the percentage of companies with a formal cyber security policy was substantially lower (see Figure 30). ICT security policy or strategy has to be translated into specific actions and practices to have an effect. One group of efforts aims to improve awareness and skills of companies employees. Across the EU, 48% of companies reported making steps to raise awareness of ICT security policy and the relevant risks. Other efforts include internal ICT security procedures and data protection. The most popular procedure was strong password authentication (min 8 characters, max 6 months, encrypted transmission and storage), which was used by 46% of companies, while 13% used hardware security tokens for user identification and authentication. Offsite data back-up, – i.e., sending critical data to another location to improve its protection – was also used by 46% of all enterprises.

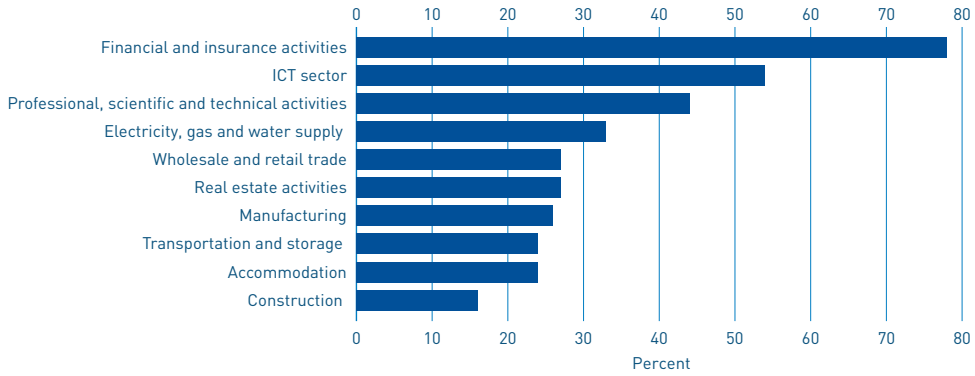


FIGURE 29 PERCENTAGE OF EU COMPANIES HAVING A FORMALLY DEFINED ICT SECURITY POLICY BY ECONOMIC SECTOR, % OF ALL ENTERPRISES (WITH 10 AND MORE EMPLOYEES). SOURCE: EUROSTAT, 2010 (DATA CODE: ISOC_CISCE_RA)

4.2.3 Citizens' concerns

The large majority of Internet users in the EU express high levels of concern about cyber security according to a recent Eurobarometer survey: 85%of them believe that the risk of becoming a victim of cybercrime is increasing.[72] 73% think that their online

personal information is not kept secure by web sites and 67% are concerned that information is not kept secure by public authorities. Almost half (47%) have experienced malicious software on their computers or other devices.

The level of knowledge about the risks of cybercrime seems to be slowly increasing in the EU: 47% of EU citizens say that they are well informed about these risks in the poll conducted in October 2014, compared to 44% in the earlier poll in May-June of 2013. An even higher percentage of Internet users – 74% – say that they are able sufficiently protect themselves against cyber crime by taking precautions or installing antivirus software.[73]

The main precautions taken by Internet users are shown in Figure 31. Installing anti-virus software was the most popular answer (61% of Internet users) but this percentage varied substantially across the EU member states. 11% of respondents say they have not made any changes because of concerns about security issues.

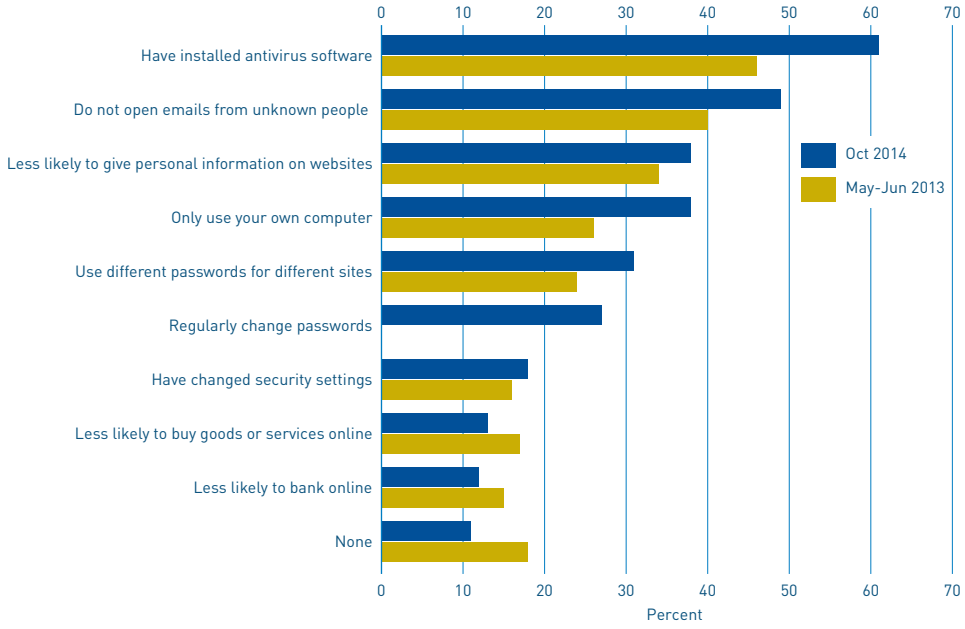


FIGURE 31 CONCERN ABOUT SECURITY ISSUES OF INTERNET USERS[74]

4.3 Cyber security expenditure

Cyber security expenditures of different actors provide a good gauge for measuring the perception of cyber security risks, the overall magnitude of cyber security activity and its evolution over time. Any organization, whether in the private or public sector, operates within budget constraints (the same statement obviously applies to individuals as well). Before it decides to spend money on improving the protection of ICT systems against cyber threats it does, at least, implicit analysis of the cost involved and benefits in terms of reduced probabilities of losses due to cyber threats. Total amount spent on cyber security is a result of independent and decentralized decision making by millions of economic agents. This is why this information provides an important insight into real perception of cyber threats and demand for IT security solutions.

Unfortunately, this data is not easy to come by. Estimates of cyber security spending (or market size) are produced most often by market research firms, which consider them as proprietary information and sell them to clients without the right to reproduce them. Even when such data is available in the public domain, it is often confusing. One reason for this is the absence of a shared definition of "cyber security." Different organizations use different definitions of this and related terms. As a consequence, the scope and boundary of the cyber security market often differ substantially. The methodologies used to estimate the cyber security market size might be quite different as well (and often are not described in any detail). All these factors lead to the situation when estimates of cyber security spending differ a lot.

One study conducted for the European Commission by IDC, a reputable market research company, divides the network and information security (NIS) market, which we assume to be the same as the cyber security market, into three main functional segments: software, services and hardware (see table below).

SEGMENT	DESCRIPTION
HARDWARE	
Hardware Authentication	It includes the hardware token market
Threat Management Appliances	It offers a combination of security software embedded into a specific hardware (Firewall + VPN)
SOFTWARE	
Identity and Access Management	A comprehensive set of solutions used to identify users in a system and control their access to resources within that system by associating user rights and restrictions with the established identity.
Security and vulnerability Management	A comprehensive set of solutions that focus on allowing organizations to determine, interpret and improve their risk posture.
Secure Content and Threat Management	This software defends against viruses, spyware, spam, hackers, intrusions, and unauthorized use or disclosure of confidential information
Other Security Software	It covers emerging security solutions and some of the underlying security functions, such as encryption tools and algorithms, that are the basis for many security functions found in other software and hardware products.
SERVICES	
Consulting	Security strategy and planning, assessment, compliance audit, architecture, analysis and review, IR and forensics
Implementation	Design, HW and SW procurement, integration of security architecture, performance testing, transition/migration, knowledge transfer.
Operations	Managed security services, hosted services, outsourced services

TABLE 4. NETWORK AND INFORMATION SECURITY MARKET SEGMENTS

SOURCE: IDC, 2009

In its report, IDC provides detailed numbers on the NIS market segments for the EU and several other major regions for a number of years (summarized in Table 5). They show that cyber security spending in the EU had been growing at an annual rate of close to 15% during the period considered. European businesses spend, on average, 10% of their IT budget on security solutions.

SEGMENT	2005	2006	2007	2008E	2009F	2010F
Hardware	751	899	1,133	1,360	1,537	1,715
Software	3,962	4,263	4,845	5,574	6,042	6,604
Services	3,329	3,963	4,778	5,752	6,332	7,253
Total	**8,042**	**9,125**	**10,756**	**12,686**	**13,911**	**15,572**

TABLE 5. EU-27 NIS TOTAL SPENDING, 2005-2010, MILLION EUR

SOURCE: IDC, 2009

Direct spending by consumers on IT security (in contrast to companies and businesses) in the EU was rather small – below 6% of the total, and this share was projected to decline further in the future. This is partly due to the fact that IT vendors pre-install some basic cyber security tools and software on computers sold to consumers.

IDC does not provide the size of the global NIS market but it gives numbers for the main geographic markets (see Table 6 below).

REGION	NIS MARKET, BILLION EUR	SHARE OF MARKET SEGMENTS:		
		HARDWARE	SOFTWARE	SERVICES
USA	13.5	13%	33%	55%
EU	10.8	11%	45%	44%
Japan	8.5	5%	24%	71%
Asia-Pacific (ex-Japan)	2.4	29%	33%	39%

TABLE 6. NIS TOTAL SPENDING BY GEOGRAPHIC REGION, 2007

SOURCE: IDC, 2009

This data is helpful but also quite outdated. More recent estimates at a more aggregate level are available from several sources that show a continuous increase in spending on cyber security. For example, in 2014 the European Organization for Security estimated the value of the global cyber security market to be EUR 56 billion, with Europe accounting for EUR 9.5 billion or 17%,[75] which is lower than IDC's estimates for 2007. Other recent estimates give a range of around USD 70-90 billion for the cyber security market value in 2014.[76] Many analysts think that the global cyber security will be among the fastest growing segments of the IT market in the next five years, growing at above 10% per year (see Table 6). It is expected to reach USD 120 billion by 2017 and USD 155 billion by 2019.[77]

The supply side of the cyber security market includes many companies providing hardware, software, and services. Some of these companies are huge multinationals such as Cisco, IBM and Microsoft but there are also many small, locally-oriented companies. The degree of concentration in the overall cyber security market is rather low. The IDC report estimated that for the EU-27 the top five vendors controlled about 20% of total market revenue in 2007, which is rather low.[78] The level of concentration was the lowest in the service segment of the market and the highest in the hardware market.

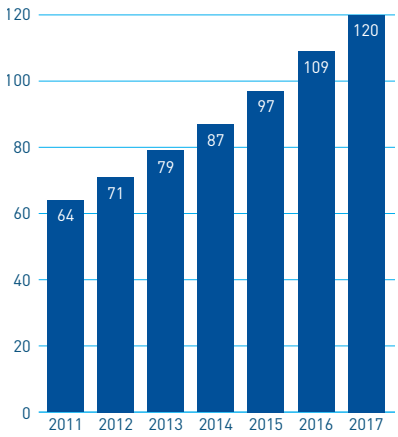


FIGURE 32 CYBER SECURITY MARKET, BILLION USD. SOURCE: MARKETSANDMARKETS, HTTP://MARKETREALIST.COM/2014/12/CYBER-SECURITY-PRESENTS-OPPORTUNITY-SYMANTEC/

Some of the largest spenders on cyber security are governments, and the U.S. federal government is likely to be the largest spender among all others. An official report finds that IT security spending at various agencies of the U.S. Federal government was USD 14.6 billion in fiscal year 2012, with the Department of Defense accounting for more than 80%.[79] Approximately 90,000 people in the US federal government had as their primary responsibility IT (cyber) security in FY2012, and 67% of them were government employees while the rest were contractors.[80]

The numbers listed in this sub-section show that cyber security is a large and growing area of IT spending for companies and public agencies. Yet the number of cyber attacks and related losses does not seem to be in decline. Therefore the question remains if existing efforts to address cyber security risks are adequate.

4.4 Overall assessment of the state of cyber security

Over the past years, various indices and rankings have been developed to provide indicators of the progress of countries on the cyber security front. However, their results should be taken with a grain of salt.

Part of the problem is the contradiction which lies at the core of cyber security: the less connected a country is to the Internet, the less reliant it is on ICT systems and infrastructure, the lower the risk of cyber threats. Limiting reliance on the Internet and ICT in general, however, is not a feasible answer, except in a very limited number of cases. It is difficult to see how countries can stay competitive in the global economy and to improve living standards of their population without realizing the benefits of ICT and increased connectivity.

Nevertheless, indices provide interesting and potentially useful information for assessing the cyber security performance of various countries. First, their methodologies illustrate how researchers formalize the notion of cyber security using various quantitative and qualitative indicators applied to a range of countries. Measuring cyber security is difficult, however comparison of different methodologies should be helpful in improving our understanding. Second, the results of such indices provide useful information and should help to get a broader picture of the state of cyber security on a country basis. Finally, a comparative analysis of the rankings, for example, to what extent they agree with each other, reveals limitations in their respective approaches.

We have identified four recently developed indices that assess cyber security capabilities and commitments of nation states. These include:

1. International Telecommunication Union (ITU) and ABI Research, Global Cybersecurity Index, 2014
2. Economist Intelligence Unit (Booz-Allen-Hamilton), Cyber Power Index, 2012
3. Melissa Hathaway, Cyber Readiness Index 1.0, 2013
4. Security and Defence Agenda (SDA), Cybersecurity Preparedness Ranking, 2012

A brief description of the methodologies is provided in the Annex. Below we analyze their results on a comparative basis.[81]

The indices that we reviewed cover a number of different countries. One way to compare their results is to look at what countries were evaluated as best performers in terms of cyber security. This information is listed in the table below. This table also provides information from the Networked Readiness Index 2014, developed by the World Economic Forum, that assesses "the progress of 148 economies in leveraging ICTs to increase productivity, economic growth and the number of quality jobs." [82]

NETWORKED READINESS INDEX, 2014	GLOBAL CYBERSECURITY INDEX, 2014	CYBER POWER INDEX, 2012	CYBER READINESS INDEX 1.0, 2013	CYBER-PREPAREDNESS RANKING, 2012
1 Finland	1 USA	1 UK	1 Netherlands, UK, Australia, USA, Canada	1 Finland, Israel, Sweden
2 Singapore	2 Canada	2 USA		
3 Sweden	3 Oman, Australia, Malaysia	3 Australia		
4 Netherlands	4 New Zealand, Norway	4 Germany		4 Denmark, Estonia, France, Germany, Netherlands, Spain, UK, USA
5 Norway	5 Brazil, Estonia, Germany, India, Japan, Republic of Korea, UK	5 Canada		
6 Switzerland	6 Austria, Hungary, Israel, Netherlands, Singapore	6 France	6 Japan	
7 USA		7 South Korea	7 Finland, Norway, Switzerland, New Zealand, France, Germany, Austria	
8 Hong Kong		8 Japan		
9 UK		9 Italy		
10 South Korea		10 Brazil		

TABLE 7 TOP COUNTRIES IN VARIOUS CYBER RATINGS. NOTE: THE TABLE LISTS TOP 10 COUNTRIES FROM EACH RANKING/INDEX UNLESS THE RANKING IS TIED. IN THIS CASE, IT INCLUDES ALL COUNTRIES WITH THE SAME RANKING/SCORE AS THOSE THAT WOULD MAKE THE 10TH PLACE.

This table already provides some interesting observations. First, only two countries – The US and the UK – are placed in the top 10 performing countries (including tied rankings) by all 5 cyber security indices. Germany and the Netherlands rank in the top-10 of 4 of 5 indices (with the Netherlands excluded from the Cyber Power Index). Four other countries – Australia, Canada, France and Japan – appear in 3 out of 5 rankings. This pattern indicates a broad agreement between the rankings on high level of cyber security in those countries. At the same time, there are some interesting differences: the Global Cybersecurity Index includes Oman, Malaysia and India in the top performing list. These countries do not appear at such positions in any other cyber security index and typically are not mentioned by experts as examples of cyber security preparedness.

To analyze rankings in a more systematic manner we selected 25 countries that are covered by most rankings. Because various rankings evaluate a different number of countries we calculated new rankings based on a country's score in the original ranking (or index). Then, to ease comparison and improve robustness of our results, we split all countries into 4 groups (quartiles) based on their place in the calculated ranking: the lowest 25% of countries (typically the bottom 5 countries unless there are ties or a smaller number of countries in the index) were assigned score 1; the next 25% of countries – score 2 and so on. The bottom group for each index (ranking) is indicated in red, the second in orange, the third in yellow. The top group is indicated in green.

	COUNTRY	THE NETWORKED READINESS INDEX 2014	CYBER READINESS INDEX 1.0, 2013	ITU, GLOBAL CYBER-SECURITY INDEX, 2014	CYBER POWER INDEX, 2013	CYBER-PREPARED-NESS	AVERAGE
1	Argentina	1	1	1	2	n/a	1,25
2	Australia	3	4	4	3	2	3,2
3	Austria	3	3	3	n/a	2	2,75
4	Brazil	1	2	3	2	1	1,8
5	Canada	3	4	4	3	2	3,2
6	China	2	2	1	1	1	1,4
7	Denmark	3	1	2	n/a	3	2,25
8	Finland	4	3	2	n/a	4	3,25
9	France	2	3	2	4	3	2,8
10	Germany	3	3	3	4	3	3,2
11	India	1	1	3	2	1	1,6
12	Indonesia	1	1	1	1	n/a	1
13	Israel	3	2	3	n/a	4	3
14	Italy	2	1	2	3	1	1,8
15	Japan	3	4	3	4	2	3,2
16	Mexico	1	1	1	2	1	1,2
17	Netherlands	4	4	3	n/a	3	3,5
18	Russia	2	2	2	1	1	1,6
19	Saudi Arabia	2	1	1	1	n/a	1,25
20	South Africa	1	1	1	3	n/a	1,5
21	South Korea	4	2	3	3	n/a	3
22	Sweden	4	2	2	n/a	4	3
23	Turkey	2	1	2	1	n/a	1,5
24	United Kingdom	4	4	3	4	3	3,6
25	United States	4	4	4	4	3	3,8

TABLE 8 RANKINGS COMPARISON. SOURCE: HCSS.

According to the analysis of these five rankings, the Netherlands, UK and US are noted as best protected. These countries are followed by Japan, Germany, Finland, Canada, Australia, South Korea and Sweden.

This table shows that the indices broadly provide a similar picture of cyber security on a country level. Still, in some cases there are substantial differences. For example, Australia and Canada are in the top quartile in the CRI and GCI but placed in the second lowest quartile in terms of cyber preparedness by the SDA. Sweden and Israel are the opposite case. In the end, this should not be surprising. Many indices rely on the subjective judgment of experts and indicators that are easier to collect. Having a law against cyber crime is an important step but it does not indicate much about a country's capability to investigate and prosecute cyber criminals, and therefore its impact on its cyber security.

In our view, cyber security indices would benefit from a more refined conceptual view of cyber security, a clear explanation of how various factors (whether these are input, process or output indicators) contribute to it, and a stronger reliance on more objective and quantifiable indicators (e.g., the number of attacks, the cost of cyber crime and spending on cyber security).

5 CONCLUSIONS

5 CONCLUSIONS

This report has provided a general assessment of cyber threats, trends, and responses to these threats. In this concluding chapter, we list the most important observations and suggest some recommendations and several next steps to take.

Threat assessment

The reports

Based on the reports assessed, we note the emerging picture is fragmented. Seven observations stand out:

- the majority of reports assessed are published by US-based organizations. About one-third come from other European countries or European organizations. 15% of studies are from other, non-European countries
- over half of the reports aim to provide a global assessment
- 57% of all studies come from private organizations, a quarter from governmental organizations, and the remainder from research organizations and one, a non-profit organization
- most reports are based on a small "n", which in case of private organizations often reflect the client-base
- the focus of attacks differs widely: some reports zoom in on data breaches, others focus on specific attacks (such as DDOS attacks), while others look at all types of attacks
- commonly used definitions and methods for reporting cyber threats are lacking. What constitutes a cyber attack, for example, is defined differently in many reports.
- many reports provide contrasting conclusions

The threats

On the level of cyber threats, all reports looking at cyber attacks which are handled and reported to CERTs, or those registering data breaches, show an increase of cyber attacks over the last few years, ranging from a few percent to a thirteenfold increase.

Type of attacks

- Most attacks are motivated by criminal, predominantly financial intent (36-60%).
- Attacks of an activist nature seem to be less common, but estimates vary widely – from over 40 percent to only a few percent.
- Espionage attacks are estimated to constitute from 5 to 25% of all attacks, and seem to be on the rise in recent years. These activities are increasingly on the radar, partly thanks to Wikileaks and revelations made by Edward Snowden.
- Cyber warfare represents a small number of reported attacks, from 0-4%.

Perpetrators

- We know very little about who is behind cyber attacks.
- Based on 5 reports, around 6 to 28% of all attacks involve insiders to the organization.
- Two organizations note that the most common location of IP addresses identified as being involved in cyber attacks are the US and China. Further assessment varies widely.
- When looking at reports focusing on specific cyber attacks:
    - Over a quarter of all cyber crime activities emanated from computers in the US, according to Symantec.
    - According to Verizon, in 2013, cyber espionage activities were emanating predominantly in East Asia (almost 50%).

Targets

- Two reports suggest that in 2013, the US and the UK experienced most cyber attacks, with the first accounting for around half of all attacks.
- Because of the small "n" and large year-on-year variation, exact estimates are difficult and show a high degree of variability.
- Based on 5 reports, the government, industry, and the financial sector stand out as main targets.

Tools and techniques

- Most reports point to malware, worms and trojans as being the most prevalent attack techniques used.
- Overall, there is little agreement on what tools and techniques are actually used most frequently and possess the most damaging capabilities.
- Varying assessments per country are likely to reflect national differences to some extent, but they also reflect the focus of CERTs themselves.

Impact

- The costs of cyber attacks is rising: McAfee estimates point to an average of over 0.8% per GDP annually, with the Netherlands and Germany topping the chart with over 1.5%.
- Two reports suggest that the impact of cyber attacks (per employee) increases with the size of the company.

Trends

We also note some trends that are mentioned in the corpus of reports.

Perpetrators

- A new exploit-trade economy is on the rise: zero-day exploit market vulnerabilities that remain secret, unpatched, and are exploited, increase the vulnerability of a large share of users.
- State actors and Organized Criminal Groups (OCGs) converge capabilities: state actors will hire OCGs or cyber-mercenaries to become part of their approach to achieve their goal.
- States are becoming actors in cyber warfare. Because of rapidly developing offensive cyber capabilities, the threat of cyber weapons becoming a central ingredient in warfare is increasing.

Targets

- Interdependencies and the Internet of Things (IoT): cascading risks and cyber eco-systems have grown so large in complexity, that the risks involved are hard to assess, and the chances of attacks cascading throughout the system increase.
- Big Data herders and trust providers become a focal point for attacks and can serve as a stepping stone to attack a certain target further in a supply chain.
- ID theft 2.0: perpetrators will focus more on 'who you are' than 'what you have'.
- GPS positioning, navigation, and timing are a weak link in critical systems.

Tools and techniques

- Increased options for anonymization (for example by using TOR networks) expands the options of perpetrators.
- IT is becoming a 'crime-as-a-service' business for criminals: criminal services that facilitate almost any type of cyber crime on a commercial basis.
- Big data also offers opportunities to hackers, for example by allowing them to effectively pinpoint organizations vulnerable to targeted spear-phishing.

- Encryption might not be able to compete with the vastly improved computing power combined with backdoors in software.
- Cyber attacks are taking place out in the open but camouflaged: increasingly, malicious cyber attacks will form a means to gain (an unfair) advantage in legitimate acts.

Response

In order to assess how countries respond to these threats and trends, we assessed cyber strategies of several governments. This meta-assessment shows:

- According to a meta-analysis of five rankings of government preparedness to cyber attacks, the Netherlands, UK and US are noted as best protected. These countries are followed by: Japan, Germany, Finland, Canada, Australia, South Korea and Sweden.
- National cyber security strategies seem to have a predominant focus on technology developments, with less focus on broader (societal, economic, etc.) trends.
- Impact focus predominantly on CI/national security/economy, but little on social aspects, or defense effects.
- On perpetrators, substantial attention paid to terrorists, while little attention is paid to activists and structural changes.

General recommendations

The picture that emerges from our meta-assessment of cyber threat analyses is one where it has become difficult to see the forrest for the trees. There clearly are a lot of reports around, but these are based on definitions and methods that are difficult to compare. In addition, these reports (and we may add: at least parts of this meta-assessment) require a level of expertise not available to the layman. We close our report with four recommendations. If we want to provide a more encompassing and comparable assessment of cyber threats, and increase awareness thereof, we should:

- In line with emerging efforts on the international level[83], develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments, allowing for more targeted investments in cyber security, on both company and government level.
- Anticipate trends and developments at an early stage to include potential new threats.
- Develop evidence based cyber security policies in line with evidence obtained via data and indicators, rather than subjective perceptions.
- Consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.

ANNEX 1: BIBLIOGRAPHY

ANNEX 1: BIBLIOGRAPHY

41st Parameter. *The Growing Threats of Cyber Crime: Five Trends and Takeaways*. 41st Parameter, June 2013. http://www.the41st.com/sites/default/files/41st-Parameter-Cyber-Crime-Whitepaper.pdf.

Ahmad, Shehzad, and Torben Sorensen. *TrendRapport*. DKCERT, December 2015. https://www.cert.dk/trendrapport2015/DKCERT_Trendrapport_2015.web.pdf.

Akamai. *The State of the internet/Q1-4 2013*. Akamai, 2013, http://www.akamai.com/stateoftheinternet/

Aniello, Leonardo, Stefano Armenia, Roberto Baldoni, Fabrizio D'Amore, Annachiara Di Paolo, Luisa Franchina, Luca Montanari, Ida Claudia Panetta, Leonardo Querzoni, and Giovanni Rellini Lerz. *2014 Italian Cyber Security Report: Awareness, Defense and Organization in the Public Sector*. CIS Sapienza, December 2014. http://www.cis.uniroma1.it/media/CIS%20Resources/2014CIS-Report-ENG.pdf.

Arbor Network. *Arbor Special Report: Enterprise Threat Landscape*. Arbor Network, 2013. http://www.brookcourtsolutions.com/documents/2013/08/arbor_wisr_enterprise_en2013.pdf.

Atlantic Council and Zurich Insurance Company. *Beyond Data Breaches: Global Interconnections of Cyber Risk*. Atlantic Council and Zurich Insurance Company, April 2014. http://www.atlanticcouncil.org/images/publications/Zurich_Cyber_Risk_April_2014.pdf

Microsoft. *Microsoft Security Intelligence Report*. Microsoft Corporations, 2014. http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_English.pdf.

Capgemini Consulting and Sogeti High Tech. *Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT*. Capgemini Consulting and Sogeti High Tech, November 2014. https://www.capgemini.com/resource-file-access/resource/pdf/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf.

Capgemini Consulting. *De zwakste schakel in de informatiebeveiliging*. Utrecht: Capgemini Consulting, September 2013. https://www.nl.capgemini.com/resource-file-access/resource/pdf/de_zwakste_schakel_in_de_informatiebeveiliging.pdf.

Capgemini Consulting. *Trends in Veiligheid 2014*. Capgemini Consulting, April 2014. https://www.nl.capgemini.com/resource-file-access/resource/pdf/trends_in_veiligheid_2014_0.pdf.

Capgeminin Consulting. *Cybersecurity: Secure Your Digital Transformation*. Capgemini Consulting, 2015. https://www.capgemini.com/resource-file-access/resource/pdf/cybersecurity_-_secure_your_digital_transformation.pdf.

Centre for the Protection of National Infrastructure. *Cyber-Attacks: Effects on UK Companies*. Oxford Economics, July 2014. http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb.

CERT-BE. *Reported Incidents 2010-2014: Figures about Incidents Reported to CERT.be*. CERT-BE, February 2015. https://www.cert.be/files/CERTbe_Statsoverview2010-2014-EN.pdf.

CERT-IN. *Annual Report 2013*. CERT-IN, March 2014.

CERT-UK: *Quarterly Report Jul-Sep-2014*. CERT-UK, February 2014. https://www.cert.gov.uk/wp-content/uploads/2014/10/CERT-UK-Quarterly-Report-Jul-Sep-2014.pdf.

CERT-UK: *Quarterly-Report Oct-Dec-2014*. CERT-UK, n.d. https://www.cert.gov.uk/wp-content/uploads/2015/01/CERT-UK-Quarterly-Report-Oct-Dec-2014.pdf.

CERT-UK. *Quarterly Report April-June 2014*. CERT-UK, June 2014. https://www.cert.gov.uk/wp-content/uploads/2014/08/CERT-UK-Quarterly-Report-01.pdf.

CheckPoint. *Check Point Security Report 2014*. CheckPoint, 2014. http://www.checkpoint.com/documents/ebooks/security-report-2014/files/assets/common/downloads/Check%20Point%20Security%20Report%202014.pdf.

Choo, Kim-Kwang Raymond. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers & Security* 30, no. 8 (November 2011): 719–31. doi:10.1016/j.cose.2011.08.004.

Clapper, James. *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, March 2013. http://fas.org/irp/congress/2015_hr/022615clapper.pdf.

CNCERT/CC. *CNCERT Annual Report 2013*. CNCERT/CC, 2013. http://www.cert.org.cn/publish/english/upload/File/CNCERT_Annual_Report_2013.pdf.

CyberEdge Group. *2014 Cyberthreat Defense Report North America and Europe*. CyberEdge Group, 2014. http://www.brightcloud.com/pdf/CyberEdge-2014-CDR.pdf.

Engineering Ingegneria Informatica. *Capital (Cybersecurity Research Agenda for Privacy and Technology Challanges): D 2.3 List of Current and Future Cyber Security Threats*. Capital (Cybersecurity research agenda for Privacy and Technology Challanges), June 2014. http://www.capital-agenda.eu/files/Deliverables/CAPITAL_D2.3_v1.13_submitted.pdf.

European Commission. *Special Eurobarometer 423: Cyber Security*. European Commission, February 2015. http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.

EUROPOL. *The Internet Organized Crime Threat Assessment (iOCTA)*. EUROPOL, 2014.

F-Secure. *Internet Security Threat Report*. F-Secure, April 2014. https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf.

Federal Financial Insitutions Examinations Council. *FFIEC Cybersecurity Assessment: General Observations*. Federal Financial Insitutions Examinations Council, 2014. http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf.

Federal Office for Information Security. *The State of IT Security in Germany 2014*. Federal Office for Information Security, 2014. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile.

Filkins, Barbara. *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*. SANS Institute, February 2014. http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.

Fortinet. *2014 Threat Landscape Report*. Fortinet, 2014. http://www.fortinet.nl/sites/default/files/whitepapers/Threat-Landscape-2014.pdf.

Garnaeva, Maria, Victor Chebyshev, Denis Makrushin, Roman Unuchek, and Anton Ivanov. *Kaspersky Security Bulletin 2014: Overall Statistics for 2014*. Kaspersky Lab, 2014. http://cdn.securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf.

Gendron, Angela, and Martin Rudner. "Assessing Cyber Threats to Canadian Infrastructure." Occasional Papers 2012 (2012): 10–01.

Georgia Institute of Technology. *Georgia Tech Emerging Cyber Threats Report 2015*. Georgia Institute of Technology, 2014. https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf.

Hartwig, Robert, and Claire Wilkinson. *Cyber Risks: The Growing Threat*. Insurance Information Institute, June 2014. http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf.

Hathaway Global Strategies LLC. *Cyber Readiness Index 1.0*. Great Falls, VA: Hathaway Global Strategies LLC, 2013. http://belfercenter.hks.harvard.edu/files/uploads/Cyber-Readiness-Index-1-0-November-2013.pdf.

IBM Global Technology Services. *IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of Cyber Attack and Incident Data from IBM's Worlwide Security Operations*. Research Report. IBM Global Technology Services, 2013. http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

IDC, *The European Network and Information Security Market: Scenario, Trends and Challenges*. A Study for the European Commission, April 2009

Information Security Forum. *Threat Horizon 2016 -on the Edge of Trust*. Information Security Forum, 2014. http://www.ciosummits.com/Threat_Horizon_2016_Executive_Summary.pdf.

Intel Security. *Net Losses: Estimating the Global Cost of Cybercrime*. Intel Security, June 2014. http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime2.pdf.

Kaspersky Lab. *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*. Kaspersky Lab, 2014. http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf.

Kaspersky Lab. *Kaspersky Security Bulletin 2013: Malware Evolution. The Top Security Stories of 2013*. Kaspersky Lab, 2013. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.

Kaspersky Lab. *The Threat Landscape: A Practical Guide from the Kaspersky Lab Experts*. Kaspersky Lab, 2013. http://media.kaspersky.com/en/business-security/kaspersky-threat-landscape-it-online-security-guide.pdf.

Luiijf, E., K. Besseling, and P. De Graaf. *Nineteen national cyber security strategies*. International journal of critical infrastructures 9, no. 1 (2013): 3-31.

Lyne, James. *Security Threat Trends 2015: Predicting What Cybersecurity Will Look like in 2015 and beyond*. SOPHOS, 2014. https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf.

ENISA. *ENISA Threat Landscape 2013: Overview of Current and Emerging Cyber-Threats*. ENISA, December 11, 2013. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014.

ENISA. *ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-Threats*. ENISA, December 2014. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats.

Marsh & McLennan Companies. *2013 Cyber Risk Survey*. Marsh & McLennan Companies, June 2013. http://poland.marsh.com/Portals/79/Documents/MARSH-Cyber-Risk-Survey.pdf.

Mateski, Mark, Cassandra Trevino, Cynthia Veitch, John Michalski, Mark Harris, Scott Maruoka, and Jason Frye. *Cyber Threat Metrics*. Sandia National Laboratories, March 2012. http://fas.org/irp/eprint/metrics.pdf.

McAfee. *McAfee Labs 2014 Threats Predictions*. McAfee, 2014. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf.

McAfee. *McAfee Labs Threats Report: Third Quarter 2013*. McAfee, 2013. http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q3-2013.pdf.

McAfee. *The Impact of Cybercrime and Cyber Espionage*, July 2013. http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf.

Melani. *Information Assurance: Situation in Switzerland and Internationally*. Melani, 2014. http://www.news.admin.ch/NSBSubscriber/message/attachments/21041.pdf.

Mennen, M.G. *National Risk Assessment 6*. Network of Analysis for Nationa Security (ANV), 2014. https://english.nctv.nl/Images/007328-nrb-6-engels-definitief_tcm92-571136.pdf.

Nationaal Cyber Security Centrum. *Cybersecuritybeeld Nederland*. Nationaal Cyber Security Centrum, October 2014. http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2014/07/10/cybersecuritybeeld-nederland.html.

National Cybersecurity and Communications Integration Center. *ICS-CERT Monitor January-April 2014*. National Cybersecurity and Communications Integration Center, n.d. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf.

National Cybersecurity and Communications Integration Center. *ICS-CERT Monitor May-August 2014*. National Cybersecurity and Communications Integration Center, 2014 https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Aug2014.pdf.

New York State Department of Financial Services. *Report on Cyber Security in the Banking Sector*. New York State Department of Financial Services, May 2014. http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.

NTT Group. *2014 Global Threat Intelligence Report*. NTT Group, 2014. https://www.dimensiondata.com/Global/Downloadable%20Documents/2014%20NTT%20Group%20Global%20Threat%20Intelligence%20Report.pdf.

OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD Digital Economy Papers, No. 211, OECD Publishing, 2012.

Pew Research Center. *Cyber Attacks Likely to Increase*. Pew Research Center, October 2014. http//www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

Ponemon Insitute. *2014 Global Report on the Cost of Cyber Crime*. Ponemon Insitute, October 2014. http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1.0.

Ponemon Institute. *2014: A Year of Mega Breaches*. Ponemon Institute, January 2015. http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

PriceWaterhouseCoopers. *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015*. PriceWaterhouseCoopers, September 2014. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

PriceWaterhouseCoopers. *US Cybercrime: Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey*. PriceWaterhouseCoopers, June 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.

Risk Based Security. *Data Breach Quick View: 2014 Data Breach Trends*. Risk Based Security, February 2015. https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf.

Robinson, Neil, Luke Gribbon, Veronika Horvath, and Kate Robertson. "Cyber-Security Threat Characterisation," 2013. http://www.rand.org/pubs/research_reports/RR235.html.

Trustwave. *2013 Global Security Report*. Trustwave, n.d. http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

Trustwave. *2014 State of Risk Report*. Trustwave, November 2014. https://www2.trustwave.com/rs/trustwave/images/2014_TW_StateofRiskReport.pdf.

Trustwave. *2014 Trustwave Global Security Report*. Trustwave, 2014. https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf.

United Nations Institute for Disarmament Research. The *Cyber Index: International Security Trends and Realities*. United Nations, 2013. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

United States of America - Department of the Army/Department of the Navy. *Cyberspace Operations*. United States of America - Department of the Army, February 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Verizon. *2013 Data Breach Investigations Report*. Verizon, 2013. http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf.

Verizon. *2014 Data Breach Investigations Report*. Verizon, 2014. http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf.

Watkins, Bryan. *The Impact of Cyber Attacks on the Private Sector*. MindPoint Group, 2014. http://www.amo.cz/editor/image/produkty1_soubory/the-impact-of-cyber-attacks-on-the-private-sector.pdf.

Websense Security Labs. *2015 Security Predictions*. Websense Security Labs, 2015. http://www.websense.com/assets/reports/report-2015-security-predictions-en.pdf.

Websense. *Websense 2014 Threat Report*. Websense, March 2014. http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf.

World Economic Forum. *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*. World Economic Forum, January 2015. http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

ANNEX 2: DETAILED OVERVIEW OF REVIEWED CYBER THREAT ASSESSMENTS

ANNEX 2: DETAILED OVERVIEW OF REVIEWED CYBER THREAT ASSESSMENTS

	AUTHOR	TITLE	ACTOR TYPE	YEAR PUBL.	YEAR ANALYSIS	GEOGRAPHICAL FOCUS	REGION OF PUBLICATION
1	CIS Sapienza	2014 Italian Cyber Security Report: Awareness. Defense and Organization in the Public sector	Academic	2014	2014	Italy	Italy
2	Georgia institute of Technology	Emerging Cyber threats report 2015	Academic	2014	2013	Global	United States
3	Kim-Kwang Raymond Choo	The Cyber threat landscape: Challenges and future research directions	Academic	2011	N/A	Global	N/A
4	University of Amsterdam	Preventing Common Attacks on Critical Infrastructure	Academic	2015	N/A	Netherlands	Netherlands
5	University of Amsterdam	Trusted Networks Initiative to combat DDoS attacks	Academic	2015	N/A	Netherlands	Netherlands
6	University of Derby	An analysis of the Characteristics of Cyber Attacks	Academic	2014	2013-2014	Global	United Kingdom
7	Canadian Security Intelligence (CSIS)	Assessing Cyber threats to Canadian infrastructure	Government	2012	N/A	Canada	Canada
8	CCNCERT/CC	CNCERT/CC Annual Report 2013	Government	2013	2013	China	China
9	Center for the Protection of National Infrastructure (CPNI)	Cyber Attacks: Effects on UK companies	Government	2014	2005-2013	United Kingdom	United Kingdom
10	CERT-BE	Reported incidents 2010-2014: Figures about incidents reported to CERT.be	Government	2015	2010-2014	Belgium	Belgium
11	CERT-UK	CERT-UK Quarterly Report	Government	2015	Q4-2014	United Kingdom	United Kingdom
12	CERT-UK	CERT-UK Quarterly Report	Government	2014	Q2-2014	United Kingdom	United Kingdom
13	CERT-UK	CERT-UK Quarterly Report	Government	2014	Q3-2014	United Kingdom	United Kingdom
14	European Commission	Cyber Security: Report	Government	2015	2014	Europe	Europe
15	European Network and Information Security Agency (ENISA)	ENISA Threat Landscape 2014: Overview of current and emerging cyber-threats	Government	2014	2013-2014	Europe	Europe
16	European Network and Information Security Agency (ENISA)	ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats	Government	2013	2013	Europe	Europe
17	EUROPOL	The Internet Organized Crime Threat assessment	Government	2014	2013-2014	Global	Europe
18	Federal Financial Institutions Examination Council (FFIEC)	FFIEC Cyber Security Assessment: General Observations	Government	2014	N/A	N/A	United States

	AUTHOR	TITLE	ACTOR TYPE	YEAR PUBL.	YEAR ANALYSIS	GEOGRAPHICAL FOCUS	REGION OF PUBLICATION
19	Federal Office for Information Security	The State of IT security in Germany	Government	2014	2014	Germany	Germany
20	Network of analysis for national security (ANV)	National Risk Assessment 6	Government	2014	N/A	Netherlands	Netherlands
21	New York State Department od Financial Services	Report on Cyber Security in the Banking Sector	Government	2014	2013	United States	United States
22	Sandia National Libraries	Cyber Threat Metrics	Government	2012	N/A	N/A	United States
23	United Nations Institute for Disarmament Research (UNIDIR)	The Cyber Index: International Security Trends and Realities	Government	2013	N/A	Global	Global
24	World Economic Forum	Partnering for Cyber Resilience: Towards the quantification of Cyber threats	Non-Profit Organization	2015	2011-2015	Global	Switzerland
25	41st Parameter	The Growing threat of Cyber Crime: Five trends and takeaways	Private	2013	2013	N/A	United States
26	Arbor Network	Enterprise Threat Landscape	Private	2013	2013	Global	United States
27	ATOS	CAPITAL: Cyber security research Agenda for Privacy and Technology Challenges: List of emerging areas of information	Private	2014	2014	Global	France
28	Akamai	State of the Internet Report	Private	2013-2014	Q1-4 2013	Global	United States
29	Capgemini Consulting	Securing the Internet of things opportunity: Putting Cyber Security at the heart of the IoT	Private	2014	2014	Global	France
30	Check Point	Security report	Private	2014	2013	Global	Netherlands
31	CyberEdge Group	2014 Cyberthreat Defense Report: North America and Europe	Private	2014	2013	North America and Europe	United States
32	F.Secure	Threat Report H1 2014	Private	2014	2014	Global	United States
33	Fortinet	2014 Threat Landscape Report	Private	2014	2013	Global	United States
33	Hackmageddon	Cyber attack statistics	Private	2012-2015	2011-2014	Global	Italy
34	Hathaway Global Strategies	Cyber Readiness Index 1.0	Private	2013	2013	Global	United Kingdom
35	IBM Global Technology Services	IBM Security Services 2014 Cyber Security Intelligence Index	Private	2014	2013	Global	United States
36	Insurance Information Institute	Cyber Risks: The growing threat	Private	2014	2013-2014	United States	United States
37	Intel Security	Net Losses: Estimating the Global Cost of Cyber Crime	Private	2014	2014	Global	United States
38	Kaspersky	Security Bulletin	Private	2015	2014	Global	Russia
39	Kaspersky	The Threat Landscape	Private	2013	2013	Global	Russia
40	Kaspersky	IT Security Risk Survey	Private	2014	2014	Global	Russia
41	Kaspersky	The Threat Landscape	Private	2014		Global	Russia
42	Kaspersky	Kaspersky Security Bulletin 2013	Private	2013	2013	Global	Russia
43	Kaspersky	Kaspersky Security Bulletin 2013	Private	2013	2014	Global	Russia
44	Marsh and McLennan co.	2013 Cyber Risk Survey	Private	2013	2013	Europe	United States

	AUTHOR	TITLE	ACTOR TYPE	YEAR PUBL.	YEAR ANALYSIS	GEOGRAPHICAL FOCUS	REGION OF PUBLICATION
45	McAfee	The Economic Impact of Cybercrime and Cyber espionage	Private	2013	N/A	Global	United States
46	McAfee	McAfee Threat Predictions 2014	Private	2014	2014	Global	United States
47	MELANI	Information Assurance - Situation in Switzerland and Internationally	Private	2014	2014	Global	Switzerland
48	Microsoft	Microsoft Security Intelligence Report, Volume 17, January-June 2014	Private	2015	Q1-2 2014	United States	United States
49	MindPoint Group	The Impact of Cyber Attacks on the Private Sector	Private	2014	2009-2013	Global	United States
50	NTT Innovation Institute	The Shifting Threat Landscape	Private	2014	2013	Global	United States
51	PriceWaterhouseCoopers (PWC)	US Cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of CyberCrime Survey	Private	2014	N/A	United States	United Kingdom
52	PriceWaterhouseCoopers (PWC)	Managing Cyber risks in an interconnected world	Private	2014	2013	Global	United States
53	SANS	Health Care Cyberthreat Report: Widespread Compromises Detected. Compliance Nightmare on Horizon	Private	2014	2014	US	United States
54	SOPHOS	Security Threat Trends 2015: Predicting what security threat will look like in 2015 and beyond	Private	2015	N/A	Global	United Kingdom
55	Symantec	Internet Security Threat Report 2014	Private	2014	2013	Global	United States
56	Trustwave	2014 Global Security Report	Private	2014	2013	Global	United States
57	Trustwave	2014 State of Risk Report: Based on a survey commissioned by trustwave	Private	2014		N/A	United States
58	Verizon	2013 Data Breach Investigations Report	Private	2013	2012	Global	United States
59	Verizon	2014 Data Breach Investigations Report	Private	2014	2013	Global	United States
60	Websense	2015 Security Predictions	Private	2015	2015	N/A	United States
61	Websense	2014 Threat Report	Private	2014	2013	Global	United States
62	Atlantic Council	Beyond data breaches: global interconnections of cyber risk	Think-Tank	2014	2014	Global	United States
63	Pew Research Center	Digital Life 2015: Cyber Attacks Likely to Increase	Think-Tank	2014	2014	United States	United States
64	Ponemon Institute	2014: Global Cost of Cyber attacks	Think-Tank	2014	2014	Global	United States
65	Ponemon Institute	2014: The Year of the mega breach	Think-Tank	2015	2014	United States	United States

ANNEX 3: OVERVIEW OF CYBER PREPAREDNESS RANKINGS

ANNEX 3: OVERVIEW OF CYBER PREPAREDNESS RANKINGS

Global Cybersecurity Index

The Global Cybersecurity Index (GCI) aims to measure the level of commitment to cyber security and the cyber security development capabilities of sovereign nation states. It looks at five categories of indicators corresponding to ITU's Global Cybersecurity Agenda (see Table 9). Each category has several indicators which are valued on the ordinal scale:

- 0 point is allocated when there are no activities;
- 1 point is allocated for partial action;
- 2 points are allocated for more comprehensive action.

The GCI scores 194 countries, which is by far the broadest coverage compared to the other indices.

CATEGORIES	VALUES
1. LEGAL MEASURES	4
A. Criminal legislation	2
B. Regulation and compliance	2
2. TECHNICAL MEASURES	6
A. CERT/CIRT/CSIRT	2
B. Standards	2
C. Certification	2
3. ORGANIZATIONAL MEASURES	8
A. Policy	2
B. Roadmap for governance	2
C. Responsible Agency	2
D. National Benchmarking	2
4. CAPACITY BUILDING	8
A. Standardization development	2

	B. Manpower development	2
	C. Professional certification	2
	D. Agency certification	2
5.	COOPERATION	8
	A. Intra-state cooperation	2
	B. Intra-agency cooperation	2
	C. Public-private partnership	2
	D. International cooperation	2

TABLE 9. GLOBAL CYBERSECURITY INDEX CATEGORIES

Cyber Power Index

The goal of the *Cyber Power Index* is to benchmark the ability of the G20 countries "to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy." The index was developed by the Economist Intelligence Unit and sponsored by Booz Allen Hamilton. It includes 39 quantitative and qualitative indicators organized into four categories (see Table 10).

CYBER POWER CATEGORIES	WEIGHT
1. Legal and Regulatory Framework	26.3%
2. Economic and Social Context	25.0%
3. Technology Infrastructure	26.3%
4. Industry Application	22.5%

TABLE 10. CYBER POWER INDEX CATEGORIES

The most relevant category for our purpose is the legal and regulatory framework, which directly deals with cybersecurity issues. The other categories have a broader character and measure more the general level of ICT adoption and application rather than specific cyber security aspects.

LEGAL AND REGULATORY FRAMEWORK	SCORE
National cyber plan	0 – 4
Public/private partnerships	0 – 4
Cyber enforcement authority	0 – 4
Cybersecurity laws	0 – 4
Cyber crime response	0 – 4
International cybersecurity commitments	0 – 4
Cybersecurity plan	0 – 4
Cyber censorship	0 – 2
Political efficacy	0 – 100
Intellectual property protection	0 – 4

TABLE 11. LEGAL AND REGULATORY FRAMEWORK INDICATORS IN THE CPI

Cyber Readiness Index 1.0

The Cyber Readiness Index (CRI) compares maturity and commitment of 35 countries in terms of protecting their investment in ICT and the Internet using an initial assessment of where countries stand in cyber security in five areas:

- National Strategy
- Incident Response
- e-crime Law Enforcement
- Information Sharing
- R&D

Cyber security preparedness ranking

A study by Security and Defence Agenda assessed the cyber preparedness of 23 countries. The ranking that was produced as a result of this study relies fully on subjective expert assessment unlike the other indices we considered. It is based on interviews with more than 80 cyber security experts from the public and private sectors, international organizations and academia. The report uses the Cyber Security Maturity Model developed by Robert Lentz for assessing resilience against cyber attacks. This model provides a five-step roadmap for improving cyber security preparedness and resilience. The steps involved start from applying basic rules of computer security hygiene to using standards, to predictive cyber readiness and supply chain risk management. This models was used as the measurement tool for assessing countries' cyber security preparedness.

ANNEX 4: TERMS AND ABBREVIATIONS

ANNEX 4: TERMS AND ABBREVIATIONS

APT	A set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.[85]
ATTRIBUTION (PROBLEM OF)	The act of determining the identity or location of an attacker or an attacker's intermediary.[86]
BREACH	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed[87]
CERT	Computer Emergency Response Team
CAAS	Crime-as-a-service
CLOUD COMPUTING	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.[88]
CYBER ATTACK	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.[89]
CYBER CRIME	Any crime that involves a computer and a network.
CYBER ESPIONAGE	The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.[90]
CYBER SPACE	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[91]
CYBER WARFARE	The actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.[92]
CRITICAL INFRASTRUCTURE	System and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[93]
DISCLOSURE	A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.[94]

(D)DOS	(Distributed) denial-of-service, an attempt to make a machine or network resource unavailable to its intended users.
ENCRYPTION	The process of encoding messages or information in such a way that only authorized parties can read it.
ENISA	European Network and Information Security Agency, is an agency of the European Union created in 2004 and located in Heraklion (Greece).
GBPS	Gigabit per second *(Gbps or Gb/s)* is a unit of data transfer rate.
GDP	Gross Domestic Product
GPS	Global Positioning System
HACKTIVISM	The subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information.
ICS	Industry Control System, a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.
ICT	Information and Communication Technology
INCIDENT	An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[95]
INSIDER THREAT	A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
INTERNET OF THINGS	The network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.[96]
IP ADDRESS	A numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[97]
ITU	International Telecommunication Union
MALWARE	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.[98]
OCG	Organized crime groups
OSI MODEL	The Open Systems Interconnection model (OSI Model) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers.
PHISHING	Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means.[99]
PNT	Positioning, navigation, and timing
RANSOMWARE	A type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

SCADA	Supervisory Control and Data Acquisition System - networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems.[100]
SPAM	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.[101]
TOR	TOR (The Onion Router) is free software for enabling anonymous communication.
TROJAN	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.[102]
TTP	Tactics, Techniques and Procedures.
WORM	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.[103]

ANNEX 5: SPONSOR OVERVIEW

ANNEX 5: SPONSOR OVERVIEW

Hoffmann Bedrijfsrecherche BV was founded in 1962 and with 80 employees it is currently the largest investigation and consultancy agency in Western Europe. Hoffmann assists organizations to protect themselves against fraud, from internal criminality to cybercrime. For this reason Hoffmann is specialized in company investigations, ICT Security and Consultancy & Training. These departments complement each other perfectly. So Hoffmann is able to answer all issues as to security and fraud completely independent.

The ICT Security department considers ICT infrastructures of organizations from the point of view of the cyber criminal in order to find out the weak spots. This enables organizations to take swift and adequate measures. Subsequently Hoffmann advises the organizations in prevention and assists in the communication and media strategy to be followed. In this way cyber criminality can be dealt with correctly, as a continuity risk! Hoffmann considers cybercrime as being one of the most serious threats for organizations now and in the future.[104]

Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. With almost 140,000 people in over 40 countries, the Group reported 2013 global revenues of EUR 10.1 billion. Capgemini has developed its own way of working, known as the Collaborative Business Experience™ and draws on Rightshore®, its worldwide delivery model.[105]

With over 2,500 professional employees, it offers a complete range of integrated cyber security services to guide and secure the digital transformation of companies and administrations. Capgemini protect your data, IT and industrial systems, and the Internet of Things (IoT). They have the resources to strengthen your defenses, optimize

your investments and control your risks. They draw on a team of security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and an R&D team that specializes in malware analysis and forensics. They have ethical hackers, five security operation centers (SOC) around the world, a licensed Information Technology Security Evaluation Facility, and are a global leader in the field of testing.

TNO[106], The Netherlands Organization for Applied Scientific Research, is one of Europe's leading independent research and development organizations. TNO is a not-for-profit organization which by law is required to operate in an independent and objective way. TNO's unique position is attributable to its versatility and capacity to integrate this knowledge, to find creative answers to the questions posed by society.

TNO innovates for a secure cyberspace; that is resilient and resistant to disruptions. A cyberspace that promotes innovation, helps the economy and enhances national security. TNO considers Cyber Security as a key enabler for digitally driven innovations, and seeks to strengthen the cyber resilience of governments, businesses and citizens. TNO's Cyber Security Lab offers promising cyber security innovation projects and the required technical facilities and workspace. TNO's vision involves an integrated and multidisciplinary approach to the challenges of Cyber Security, with emphasis also on the role of humans, processes, organization and governance.

The NLnet foundation[107] stimulates network research and development in the domain of Internet technology. The articles of association for the NLnet foundation state: "to promote the exchange of electronic information and all that is related or beneficial to that purpose". However, last year's increasing issues with respect to cybersecurity-threats have virtually translated our mission in "maintaining the Internet as originally envisioned". NLnet does not directly benefit from the undertaken projects, and most developments are public domain.

The Hague Security Delta (HSD)[108] is the largest security cluster in Europe. In this Dutch cluster, businesses, governments, and knowledge institutions work together on innovation and knowledge in the fields of cyber security, national and urban security, protection of critical infrastructure, and forensics. They

share a common goal: more business activity, more jobs, and a secure world. The security cluster originated in The Hague, where the HSD Campus, the national innovation centre for security, is also situated. The regions Twente and Brabant contribute to this in particular with their innovative living labs and universities. The main focus areas of the region The Hague are: cyber security, forensics, national security, and critical infrastructure.

The Municipality of the Hague is the capital of the province of South-Holland. The Dutch government and parliament are situated in the city and it serves as residence of the Royal Family. The Hague is also the International City of Peace and Justice. It is the United Nations' second city, after New York. There are 160 international organizations in The Hague, employing around 14,000 people dedicated to the cause of world peace.

ENDNOTES

ENDNOTES

1 This can capitalize on ongoing discussions in international fora such as the UN, NATO and the World Economic Forum.
2 Ibid.
3 Ibid.
4 Verizon, 2014 Data Breach Investigations Report. 2014, p 8.
5 Ibid.
6 The full overview of all reports is available in the Annex.
7 IBM. *IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of Cyber Attack and Incident Data from IBM's Worlwide Security Operations*. Research Report. IBM Global Technology Services, 2014, p 4.
8 Hoffmann. *Top-5 zwakheden ICT beveiliging*. September 2014. Available at https://www.hoffmannbv.nl/over-ons/nieuws/persbericht-lekken-van-informatie-top-5-zwakheden-de-ict-beveiliging
9 Gantz, John, and David Reinsel. *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East*. IDC, 2012.
10 "Cyber Crime and Security Survey Report 2012," CERT Australia, https://www.cert.gov.au/system/files/614/679/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf: 5.
11 Melani. *Information Assurance: Situation in Switzerland and Internationally*, 2014.
12 See for example http://www.wired.com/2014/03/bitcoin-exchange.
13 M-Trends, 2015
14 Ibid.
15 Data available at http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
16 Van Kessel, Jeroen, and Alexandros Stavroulakis. "Trusted Networks Initiative to Combat DDoS Attacks." University of Amsterdam, 2015.
17 Europol. The Internet Organized Crime Threat Assessment, 2014.
18 See for example SOPHOS. *Security Threat Trends 2015: Predicting What Cybersecurity Will Look like in 2015 and beyond*. 2014
19 Symantec Corporation. *Internet Security Threat Report*. April 2014.
20 Canadian Security Intelligence Service, Assessing Cyber Threats To Canadian Infrastructure, 2012
21 SOPHOS. *Security Threat Trends 2015: Predicting What Cybersecurity Will Look like in 2015 and beyond*. 2014.

22 Symantec Corporation. *Internet Security Threat Report*. April 2014.

23 NTT. *2014 Global Threat Intelligence Report*. NTT Group, n.d.

24 SOPHOS. *Security Threat Trends 2015: Predicting What Cybersecurity Will Look like in 2015 and beyond*. 2014.; and Director of US National Intelligence, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, 2013.

25 Hathaway, Melissa E. "Cyber Readiness Index 1.0." *Great Falls, VA: Hathaway Global Strategies LLC*, 2013.

26 McAfee and CSIS. Net Losses: Estimating the Global Cost of Cybercrime. June 2014.

27 See for example http://www.newsweek.com/2014-year-cyber-attacks-295876, http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

28 See for example http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

29 http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003

30 See for example http://ijsr.net/archive/v3i3/MDIwMTMxMjAx.pdf

31 See for example http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/

32 See for example http://www.zdnet.com/article/rsa-brazils-boleto-malware-stole-nearly-4-billion-in-two-years/ http://www.emc.com/collateral/white-papers/h13282-report-rsa-discovers-boleto-fraud-ring.pdf

33 See for example http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/, http://www.newsweek.com/2014-year-cyber-attacks-295876, http://www.coughlinduffy.com/uploads/29/doc/UNDER_ATTACK_-_THE_DELUGE_OF_CYBER_ATTACKS_AND_INDUSTRY_RESPONSE.pdf

34 See for example http://www.ibtimes.co.uk/sony-pictures-hack-recovering-cyberattack-will-cost-company-15m-1486567, http://www.cnet.com/news/sony-pictures-hack-to-cost-the-company-only-15-million/

35 By looking at societal development and technology trends from the perspective of the perpetrator, the target and the tools and techniques, we can present a broad view of the cyber threats and trends. It should be noted that separating trends into three neatly organized groups listed above often is not straightforward. Many technology developments create new vulnerabilities, new sets of targets or even perpetrators. We tried to minimize repetition in such cases by mentioning the development only once.

36 See for example Tegenlicht documentary - Zero days, 2014

37 https://www.schneier.com/blog/archives/2012/06/the_vulnerabili.html

38 Mandiant. M-Trends, 2015.

39 Usually also called Advanced Persistent Threats (APTs), being a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives [source: http://en.wikipedia.org/wiki/Advanced_persistent_threat].

40 See for example Joint Publication 3-12 – Cyberspace Operations, 2013] [Netherlands Defense Cyber Strategy, 2012.

41 41st Parameter. The Growing Threats of Cyber Crime, Five Trends and Takeaways, 2013.

42 Europol - The Internet Organized Crime Threat Assessment, 2014.

43 CAPITAL Project EU - Deliverable: D 2.1 List of Emerging Areas of Information Technology, 2014.

44 http://www.computerworld.com/article/2511039/cybercrime-hacking/rsa-spearphish-attack-may-have-hit-u-s--defense-organizations.html.

45 ISF, Threat Horizon 2016, 2014.

46 Canadian Security Intelligence Service, Assessing Cyber Threats To Canadian Infrastructure, 2012

47 NCSC - Cyber Security Assessment, 2014.

48 Atlantic Council & Zurich Insurance Company - Risk Nexus - Beyond data breaches: global interconnections of cyber risk, 2014.

49 Symantec Corp - Internet Security Threat Report, 2014.

50 SANS USA, Health Care Cyber threat Report, Widespread Compromises Detected, Compliance Nightmare on Horizon, 2014.

51 http://www.reuters.com/article/2014/05/29/us-rapid7-radcliffe-idUSKBN0E929K20140529.

52 Europol. The Internet Organized Crime Threat Assessment, 2014.

53 See for example http://www.dailydot.com/politics/tor-dark-net-study-size.

54 ISF. Threat Horizon 2016, 2014.

55 Europol. The Internet Organized Crime Threat Assessment, 2014.

56 See for example https://www.cqure.nl/kennisplatform/cybercrime-as-a-service/

57 Europol. The Internet Organized Crime Threat Assessment, 2014.

58 White House, National Strategy to Secure Cyberspace, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

59 ENISA, National Cyber Security Strategies in the World, at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (accessed on March 10, 2015).

60 Luiijf, E., K. Besseling, and P. De Graaf. "Nineteen national cyber security strategies." *International journal of critical infrastructures* 9, no. 1 (2013): 3-31.

61 Ibid.

62 OECD, "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, 2012.

63 Ibid, p.22.

64 Robinson, N., et al. *Cyber-security threat characterisation: A rapid comparative analysis,* RAND, 2013.

65 Ibid., p. viii.

66 Luiijf, Besseling, and De Graaf (2013).

67 Robinson, N., et al. (2013).

68 OECD, 2012.

69 This data come from Eurostat's survey carried out in 2010. Although somewhat outdated it still provides useful information , in particular for comparative purposes.

70 Eurostat uses the term "ICT security", which we will interchangeably with cyber security in this chapter.

71 Eurostat, "ICT Security in enterprises", http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises. Data from February 2011.

72 Eurostat,2010, online code: isoc_cisci_co

72 Eurobarometer 390, 2012.

73 Ibid.

74 Eurobarometer, 2013, 2014

76 Gartner, "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware", August 22, 2014, at http://www.gartner.com/newsroom/id/2828722

77 MarketsandMarkets, "Cyber Security Market worth $155.74 Billion by 2019", 2014, http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

78 IDC, 2009

79 Executive Office of the President of the United States, Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002, Washington DC, March 2013. https://www.fismacenter.com/fy12_fisma.pdf These numbers do not include some small agencies of the US federal government.

80 More precisely, the report indicates the number of Full Time Equivalents.

81 See Annex for an overview.

82 Available at http://www.weforum.org/reports/global-information-technology-report-2014

83 This can capitalize on ongoing discussions in international fora such as the UN, NATO and the World Economic Forum.

84 Not Available

85 https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

86 Institute for Defense Analyses, Techniques for Cyber Attack Attribution, October 2003.

87 ISO/IEC 27040 http://www.iso.org/iso/catalogue_detail?csnumber=44404

88 Committee on National Security Systems, National Information Assurance (IA) Glossary, 26 April 2010, (CNSSI-4009)

89 CNSSI-4009

90 http://www.oxforddictionaries.com/definition/english/cyberespionage

91 CNSSI-4009

92 http://www.rand.org/topics/cyber-warfare.html

93 CNSSI-4009

94 Verizon, 2014, p 8.

95 CNSSI-4009

96 Wikipedia

97 Wikipedia

98 CNSSI-4009

99 CNSSI-4009

100 CNSSI-4009

101 CNSSI-4009

102 CNSSI-4009

103 CNSSI-4009

104 https://www.hoffmannbv.nl/

105 http://www.capgemini.com/cybersecurity

106 www.tno.nl

107 www.nlnet.nl

108 https://www.thehaguesecuritydelta.com/

The Hague Centre for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
HCSS.NL