CRN REPORT

Focal Report 6

Assessing Threats in Cyberspace:

Interrogating methodological approaches & the challenges of today's complex risk environment

Zurich, November 2011

Risk & Resilience Research Group
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Purpose: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with compiling 'focal reports' (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and provide information about new trends and insights.

Authors: Gabriel Brönnimann, Thomas Gartmann,
Jennifer Giroux, Manuel Suter, Myriam Dunn Cavelty

Contact:
Center for Security Studies
ETH Zürich
Haldeneggsteig 4, IFW
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting entity: Federal Office for Civil Protection (FOCP)
Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination FOCP
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision ETH-CSS: Myriam Dunn Cavelty, Risk & Resilience Research Group,
Andreas Wenger, Director CSS

Disclaimer: The views expressed in this focal report do not necessarily represent the official position of the Swiss Federal Office for Civil Protection, the Swiss Federal Department of Defence, Civil Protection, and Sport or any other governmental body. They represent the views and interpretations of the authors, unless otherwise stated.

CONTENTS

FOCAL REPORTS: THE TASK

In support of Switzerland's critical infrastructure protection (CIP) efforts and CIP strategy development, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with producing focal reports (Fokusberichte) on critical infrastructure protection. These focal reports are compiled using the following method: First, a 'scan' of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process based on the following sources:

- Internet Monitoring: New publications and documents with a) a general CIP focus and b) a focus on scenarios with specific importance for the FOCP are identified and collected.
- Science Monitoring: Relevant journals are identified and regularly evaluated (with the same two focal points as specified above).
- Government Monitoring: The focus is predominantly on policy developments in the United States, Canada, Sweden, Norway, Germany, the Netherlands, and the United Kingdom as well as other states in the European vicinity that are relevant to Switzerland.

Second, the material collected is filtered, analyzed, and summarized in the focal reports.[1]

1 Previous focal reports can be downloaded from the website of the Center for Security Studies (*http://www.css.ethz.ch*). The *www.crn.ethz.ch* website will cease to exist.

INTRODUCTION

This report examines and compares publically available public and private cyber threat reports so to identify similarities and differences in threat assessment methodology, audience, and purpose. Overall, our findings observe a shift from the (near exclusive) use of quantitative methods to a mixed-method approach that increasingly favors qualitative methods – such as anecdotal evidence and in-depth case studies – to assess and communicate cyber incidents. Though quantitative methods are still widely used and highly valuable in the area of cyber threat analysis, this methodology has some limits due to the nature of the environment – one where the threat landscape in cyberspace[2] is dynamic and complex due to its constantly changing and evolving tendencies. Such characteristics create a large degree of uncertainty that can result in an information deficit. When paired with qualitative methods, however, cyber threat reports can offer more in-depth analysis on specific cases and overarching trends.

To unpack this trend, section 1 begins by comparing selected, publicly available cyber threat reports released in 2010–2011 by both the public and private sector (four from each sector). We first assess the similarities and differences, and then focus on a more detailed critique of quantitative and qualitative approaches – particularly describing the criticisms that have been levied against the use of quantitative methods. Following this, we utilize specific examples to highlight the growing role that qualitative methods are playing in assessing and understanding cyber threats. This shift to a so-called 'mixed-method approach' is embedded in a broader trend described in section 2 that positions this trend within the discussion on complex systems; arguing that cyberspace represents a complex system and securing this domain is in itself a complex task. Using this approach enables us to anchor the methodological shift as well as provide some insights on managing and assessing cyber threats, in particular with regards to the critical infrastructure (CI) debate. Finally, we conclude with a discussion that provides recommendations for Switzerland – noting that cyber threats will continue to be a complex risk for CI sectors. Rather than adopting the false mindset that all attacks are preventable, we suggest that the major challenge ahead will be to enhance the resiliency of systems as well as to develop a sound risk communication strategy that acknowledges the uncertainty, complexity and vulnerability within this domain.

2 Cyberspace can be defined as "any process, program, or protocol relating to the use of the Internet, or an intranet, for data processing, transmission, or use in telecommunication," see: United States. 2003. The National Strategy to Secure Cyberspace. Available at *http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf*.

1. ASSESSING CYBER THREAT REPORTS

For our analysis, we examined publically available cyber threat reports published by the public and private sectors in 2010–2011; with four reports (listed in Table 1) chosen from each sector. For the private sector we focused on well-established companies in the computer industry, whereas in the public sector we looked at government bodies that have a history of producing cyber threat reports, typically within the framework of protecting critical infrastructure (both physical assets and information networks). To give structure and symmetry to our analysis, we looked at sources of data (i.e. where does the content come from), audience (who is the report addressed to), content (what threats are addressed, and more importantly, in what way are they presented), purpose (stated and/or inferred), and methodology (how are threats are assessed). It bears mentioning that in comparing these two domains we did not utilize threat-specific reports but at times make reference to them.[3]

Private Sector Reports	Public Sector Reports
Microsoft Security Intelligence Report	Switzerland, Informationssicherung: Lage der Schweiz und international
Symantec Internet Security Threat Report	Germany, Die Lage der IT-Sicherheit in Deutschland
Panda Security annual report	United Kingdom, The Cost of Cybercrime
Sophos Security Threat Report[4]	United States, 2010 Internet Crime Report[5]

Table 1: Private and public sector cyber threat reports used for this study

3 The exception being the UK's non-annual threat report which focuses on the financial aspects of various cyber threats.

4 Microsoft Security Intelligence Report Volume 10: An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in 2010; Symantec Internet Security Threat Report: Trends for 2010; Annual Report PandaLabs 2010 and Sophos Security Threat Report 2011. See bibliography for details.

5 Switzerland: Informationssicherung: Lage in der Schweiz und international. Halbjahresbericht 2010/II (Juli – Dezember); Germany: Die Lage der IT-Sicherheit in Deutschland 2011. Bundesamt für Sicherheit in der Informationssicherheit; United Kingdom: The Cost of Cybercrime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. Cabinet Office; USA: Internet Crime Complaint Center: 2010 Internet Crime Report. See bibliography for details.

Despite the public nature of the reports, we found some interesting similarities and differences between the two sectors (for a comprehensive overview of the selected threat reports and their main characteristics, see Table 2). **First**, in terms of the **private sector** reports, there was a certain commonality in overall purpose and targeted audience. Broadly speaking, these companies used such publications to promote products and services that provide detailed, privileged, in-depth and specifically tailored threat information to their customers. For example, Microsoft states that their "report is designed to give our customers, partners, and the industry a better understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity".[6] This is clear even in reports that do not explicitly mention the addressed parties. Overall, this brings to light an important aspect of such reports: Dealing with cyber threats is at the core of their business model. Consequently, the information published in these firms' *free* security reports have to be read with the knowledge that although they might provide informative overviews of current threats, they are also released under the umbrella of marketing the companies' work, which may introduce some bias.[7] To note, Symantec acknowledges the reports' usefulness for its own financial goals in the introduction, stating "of course, the insights from this survey provide a strategic market outlook for Symantec. At the same time, however, sharing its results with the industry in general and IT professionals in particular will help provide benchmarks for assessing the state of their own cybersecurity readiness".[8] While it certainly would go too far to claim that data is distorted in such reports, the possibility of exaggerated threats must not be discarded. Consider, another example, McAfree's "Virtual Criminality Report 2009", which was ominously subtitled "Virtually Here: The Age of Cyberwar". Though the authors state it is "not to create hype or stoke unwarranted fear", the report goes on to make rather strong statements, such as: "The Private Sector in the Crosshairs: The threat to private companies and citizens is real. Nation-states have contemplated launching cyber attacks that could be far more devastating than what was seen in Estonia or Georgia".[9]

Second, turning to the **public sector** reports, we found that, with the exception of the Swiss report,[10] the three public sector cases used in this analysis provide annual reports on cyber threats. Unlike the private sector, however, the public sector reports have slight variance in purpose and audience (stated or inferred). For example, each report is partly focused on the distinct threat and security situation in their respective country, reflecting on trends, possible implications of threats, and future perspectives. As for audience, Switzerland's Information Assurance Centre MELANI addresses "private computer and Internet users, as well as small and medium sized businesses (SMBs)"[11] with the objective to educate computer users and small businesses about the current threats and create awareness so to mitigate risks. Although it does not state explicitly, the German BSI (Federal Office for Information Security) report basically serves

6 Microsoft, 2011, p. 11.

7 The abundance of private sector surveys and reports is not free from fundamental criticism: "While vendors say these surveys and reports are meant to alert IT professionals to growing security threats and to help vendors determine what sorts of products customers need, in fact they're creating a thick layer of fear, uncertainty and doubt, [...]that helps sell products [...]." See Garretson, Cara and Messmer, Ellen (2006): "It's raining IT security surveys". Network World, Available at http://www.networkworld.com/news/2006/032006-security-surveys.html.

8 "2011 State of Security Survey: Global Findings," Symantec (2011), p. 3. Available at: http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf.

9 "Virtual Criminality Report 2009: Virtually Here: The Age of Cyberwar," McAfree (2009), p.14. Available at: http://www.mcafee.com/in/resources/reports/rp-virtual-criminology-report-2009.pdf

10 Switzerland's Information Assurance Centre MELANI publishes two reports per year. For more information see: Reporting and Analysis Centre for Information Assurance, Available at: http://www.melani.admin.ch

11 http://www.melani.admin.ch.

the same purpose.[12] While not all-encompassing, a very broad range of different threats is discussed in both reports as well as the need for effective counter measures to include public private partnerships and end user education. As for data, MELANI relies on various sources, ranging from different security reports, online news articles, as well as its own insights and experiences with cyber threats. Likewise, the German report also uses its own sources as well as external information and lists them in a bibliography. In contrast, the US report produced by the Internet Crime and Complaint Center (IC3) serves as both a "repository for victim complaints" and "conduit for law enforcement to share information and pursue cases that often span jurisdictional boundaries."[13] Thus its data comes from the complaints and incidents sent to IC3. Yet, in the United Kingdom's (UK) report we found some notable distinctions. For one, it focuses explicitly on the financial losses caused by cyber attacks; specifically putting a price tag on how various cyber threats impact the UK's economy. This is considered as an important aspect because "estimates of the cost of cyber-crime have until now failed to address the breadth of the problem and have not been able to provide a justifiable estimate of economic impact".[14]

Pooled together, while the Swiss and German cases refrain from focusing on certain sectors over others or quantifying the impact of threats, the UK report clearly does. The US case also engages in some quantifying of impact but not to the degree seen in the UK case. Indeed, with its focus on and calculation of the financial aspects of cyber threats, the UK's report is unique. In all of the other reports, regardless of sector, there is a reluctance to use exact financial data, and, with the exception of the Microsoft report, to provide too much quantitative data on threats. This reluctance may well be explained by the criticism that purely quantitative threat surveys and reports have received in recent years and one that we will discuss in the following section as we delve more deeply into the discussion on methodology. Here, we find one notable observation: While the private sector tends to lean more towards quantitative analysis, qualitative methods are emerging as a powerful component for cyber threats analysis – this includes providing anecdotal evidence and in-depth case studies on cyber incidents.

12 BSI specifically states that its objective is "to promote IT security in Germany. The BSI is first and foremost the central IT security service provider for the federal government in Germany. However, we also offer our services to IT manufacturers as well as private and commercial users and providers of information technology because effective security is only possible when everyone involved contributes." For more see: *https://www.bsi.bund.de/EN/Home/home_node.html*.

13 USA: Internet Crime Complaint Center: 2010 Internet Crime Report, p.4. Available at: *http://www.ic3.gov/media/annualreport/2010_ic3report.pdf*

14 "The Cost of Cybercrime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office", United Kingdom Cabinet Office, Detica (2011), p.2. Available at: *http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf*.

Report Name	Sources of data	Audience	Content	Purpose
Microsoft Security Intelligence Report	In-house data collected through Microsoft services and programs	Consumers, customers, partners, the industry	Quantitative analysis of threat data collected by Microsoft; Quantitative threat overviews for countries	Provide detailed, quantitative and technical overview on current threats
Symantec Internet Security Threat Report	In-house data collected through Symantec's "global network"	Consumers, customers, partners, the industry	Five in-depth articles on current threat categories (targeted attacks, social networking/engineering, zero-day-vulnerabilities, attack kits and mobile threats)	Provide information about current threats, highlight examples & best practices for avoiding certain scams
Sophos Security threat report	In-house data from Sophos' "Collective Intelligence Database"	Consumers, customers, partners, the industry	Introduction to different threats, providing detailed explanations and examples, figures and statistics	Provide information on various current threats as well as guidance on how to counter threats
Annual Report PandaLabs	In-house data from PandaLabs, news sources, surveys	Consumers, customers, partners, the industry	Descriptions of current cybersecurity issues via small articles on specific threats. Main focus on the threats' qualitative aspects. Provide list of possible future threats	Provide information on current threats for enhanced protection
Switzerland: Informationssicherung: Lage in der Schweiz und international, 2010/II	Various sources (news articles, technology reports, own research)	Private computer and Internet users; small and medium sized businesses (SMBs)	An overview about various national and international cyber threat occurrences and threat categories. Also, prevention strategies are discussed	Providing information on current threats and thereby contributing to threat prevention
Germany: Die Lage der IT-Sicherheit in Deutschland, 2011	Various sources (own government research and statistics, technology reports and news articles)	Private computer and Internet users; small and medium sized businesses (SMBs)	An overview about various cyber threat occurrences and categories	Explaining current threats in detail and providing threat prevention strategies for readers
United Kingdom: The Cost of Cybercrime, 2011	Various economic sources and estimates	Government and business sector	Giving an estimate on the exact financial impact of cybercrime for the UK	Alerting businesses and the government to the high costs of cybercrime
United States: Internet Crime Complaint Center: 2010 Internet Crime Report	Own data collected by the Crime Complaint Center	Any parties interested in the Crime Complaint Center's annual work and statistics	An overview of the Crime Complaint Center's activities. Analysis of more than 300 000 complaints about cyber threats	Explaining some of the more common threats and providing strategies to prevent falling victim to cyber threats

Table 2: Similarities and Differences

1.1 Quantitative vs. Qualitative Approaches

In comparing methodological approaches, we found that the public sector tends to lean more towards utilizing *qualitative* methods to assess and communicate threats, whereas the private sector rely more heavily on *quantitative* methods. Yet, interestingly, as we describe in this section, the private sector reports are increasingly incorporating qualitative methods into their reports; a trend which points to the growing popularity and utility of a mix-method approach. Of course, one might be quick to assume that given the nature of publicly available reports (to be broadly assessable, and to also serve a communication function) it would make sense for analysis to be tailored for both technical and non-technical backgrounds. While this is partly true, it is also true that the exclusive use of quantitative methods to assess cyber threats has met increasing criticism and limitations in recent years. Going forward, we first look more closely at these criticisms and then explore the growing role that qualitative approaches are playing in the *assessment* and, perhaps more importantly, the *communication* of cyber threats.

1.1.1 *Quantitative Approaches – A Traditional Approach Meets Criticism*

During the 1990s, as cyber security concerns gained traction, quantitative methods were typically viewed as the best approach to assess cyber threats to information networks. Regardless of the sector, the primary objective was to use data on *past* acts to estimate current and *future* risks. In simple terms, this basically meant that cyber security professionals were counting incidents to calculate the costs from intrusions and assess prevention efforts. In fact, until 2005, knowing *how many* and *which kind* of incidents occurred was seen as a sound basis to estimate frequency and distribution of future incidents. Keeping track of attacks coupled with estimating the damage (operationalized as monetary losses) that an average attack would cause was, in theory, seen as sufficient for predicting future developments, risk levels and adopting appropriate prevention measures. This approach, however, has met growing criticism,[15] with two major issues of concern: on the one hand, data collection and sampling and, on the other hand, the operationalization of threats as costs.

First, the general critique with data collection and sampling has been that such methods lead to flawed assessments given the dynamic and rapidly changing nature of the information technology (IT) security landscape. The key argument has been that such activities would never be able to make significant comparisons over time nor provide any reliable predictions due to the constant behavioral shifts in this domain.[16] The nature of the system – one that is complex and constantly changing – hinders the ability to detect *all* attacks, which are typically carried out to avoid detection. For example, the Stuxnet virus, which has been branded as a "cyber missile", was launched in 2009 though not detected until 2010 by VirusblokAda, a Belarus-based security company.[17] By (allegedly) targeting SCADA (supervisory control and data acquisition) systems in the Iranian nuclear program, Stuxnet was able to manipulate nuclear centrifuges by feeding false data and orders to the systems controls, causing the system to be slowly damaged by either slowing down the centrifuge process or causing it to surge. Furthermore, as the timeline indicates, Stuxnet was able to hide from detection for some time before it was discovered. Highlighting the concern raised by this case, a 2011 Chatham House

15 Winkler, Ira. "Time to end the FBI/CSI study?" Computerworld, 26 September 2006. Available at: http://www.computerworld.com/s/article/9003640/Time_to_end_the_FBI_CSI_study_and_Baker, Wade H. and Wallace, Linda (2007), "Is Information Security Under Control? Investigating Quality in Information Security Management", Security & Privacy, IEEE 5:1, p. 36–44.

16 We further discuss these characteristics in section 2.

17 The Economist, "A cyber-missile aimed at Iran?" 24 September 2010. Available at: http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

study noted that, "the discovery of Stuxnet virus in 2010 provided evidence of the growing sophistication of cyber threats and the potential damage they could cause to governments, organizations, and critical infrastructure around the world."[18] In another example, in August 2011, McAfee released the report "Operation Shady RAT", which documented a five year long targeted cyber attack on the systems of various governments, the United Nations, and large companies from various industries. Comparably, while Stuxnet may be labeled sabotage, Operation Shady RAT can be classified as cyber theft and espionage.[19] Both, however, were similar in that they were able to avoid detection and successfully penetrate various systems.

Another issue concerns the use of surveys to collect information on threats to computer security (renowned examples include the *Computer Security Institute* (CSI) and specific publication outlets such as *Information Week and Information Security*). Over time, such surveys revealed high variance in findings that led to numerous contradictions between reports.[20] This is understandable considering that most (if not all) of such surveys are not representative of any group. For example, the choice of samples seldom has any theoretical foundation as many surveys do not differentiate between the varying size of companies or the business sectors.[21] Without such a differentiation the calculation of average frequency of attacks is questionable.[22]

Second, operationalizing the threats as costs also raises reliability issues. This method pertains to the tendency to look at past cyber-attacks and estimate the costs incurred from those intrusions. For instance, the 14th Annual CSI Computer Crime and Security Survey showed that:

> "[...] respondents suffered, on average, $234,000 in losses due to security incidents from July 2008 to June 2009. This is a 19 percent drop from last year's average of $289,000; which was a 16 percent drop from 2007's average of $345,000".[23]

Remarkably, this report then goes on to discredit its own findings, stating that "despite anonymity, only 102 respondents to the CSI survey (less than 25 percent) were willing to share details of their financial losses" – hardly a statistically significant number. Also, according to the 2009 CSI Report,[24] the Ponemon Institute calculated an average loss per respondent of US $6.6 million, whereas the CSI found no losses over US $6 million for the same period. The report admits that this must be due to "differences in our survey pool" – putting in doubt not only the validity and usefulness of its own cost estimates, but, by associa-

18 Cornish, Paul et al (2011). "Cyber Security and the UK's Critical National Infrastructure." A Chatham House Report, September 2011.

19 Alperovitch, Dmitri (2011). "Revealed: Operation Shady RAT," McAfree, White Paper. Available at: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

20 Computer Security Institute (2009). "14th Annual CSI Computer Crime and Security Survey, Comprehensive Edition," Computer Crime and Security Survey report, December, pp. 13–15. Available at: http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf. For some of the problems concerning the validity of data from cyber threat surveys, see Soo Hoo, Kevin J. (2000). "How Much Is Enough? A Risk-Management Approach To Computer Security. Consortium for Research on Information Security and Policy (CRISP), Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4127&rep=rep1&type=pdf, especially p. 29–46.

21 Some security bloggers have even ridiculed the CSI/FBI reports, calling it "humorous relief" because of not being based on "statistically solid" numbers and therefore dismissing it because they see the survey methods as flawed to the point where "there is no reason to give this survey any credence". See Walsh, Chris (2006): CSI/FBI survey considered harmful. Available at: http://emergentchaos.com/archives/2006/07/csifbi-survey-considered-harmful.html and Chuvakin, Anton (2006). "On 2006 CSI/FBI survey." Available at: http://chuvakin.blogspot.com/2006/07/on-2006-csifbi-survey.html.

22 Guillot, Alexis and Kennedy, Sue (2007). "Information Security Surveys: A Review of the Methodologies, Critics and a Pragmatic Approach to their Purposes and Usage," Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, p. 66f.

23 CSI (2009), p. 13.

24 Ibid, pp.13–15.

tion, Ponemon's data as well. These diverse results reveal that the task of putting an average (or even, in single cases, a precise) price tag on damage caused by cyber-attacks may well be next to impossible. Moreover, such attempts have been called "a highly speculative activity", not only because some data is in itself difficult to quantify (in terms of value), but also because it depends upon who is in possession of the information. As Soo Hoo remarks, "sensitive commercial R&D information in the hands of a competitor is significantly more problematic than if it were in the hands of a Netherlands teenager."[25] The unfortunate tendency is for most studies to provide estimates of losses that give (false) impression of accuracy even though there is a high probability of inaccuracy. This, of course, can lead to poor decisions about security measures.

Regardless of the aforementioned critiques, quantitative methods are still widely used – especially by the private sector. This is not surprising, given that numbers, or rather data, suggest a *certainty* about the threat that many decision-makers desire. For example, take the private sector, which is able to use (in-house) data gathered through their technologies and products. Microsoft, for instance, boasts the "most comprehensive and detailed perspective on the threat landscape available in the software industry" stemming from the various Microsoft-owned services and programs installed on millions of computers.[26] In addition, its 2010 analysis is presented as an "in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software", using quantitative methods in much of its reporting.[27] Given the size of this privately-owned company in the computer industry, Microsoft is able to collect data from a reported 600 million computers worldwide, which is then used to identify:

- the change of global infection rates in different countries
- trends in the frequency of occurrence within different threat categories
- the type of rogue/scareware variants and spam that were most often seen during the year
- overall worldwide infection rates per country.[28]

Likewise, Symantec states that it has compiled its report using "some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network [...]", with "intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products".[29] Panda Security uses a bit softer language, alluding to "data in our Collective Intelligence database",[30] while Sophos Security lists internal (Naked Security, SophosLabs) and external sources (various security news outlets).[31] Sophos additionally relies on security related surveys it conducts regularly. The reports are all therefore based on large data collection of various threats and, as we have highlighted through anecdotal evidence, attempt to bestow a certain confidence with such methods.

The use of quantitative methods in the public sector reports is not as common but there are some notable exceptions. The United Kingdom (UK), for instance, recently published a cyber-threat report that uses a quantitative approach. The collaborative study between the Cabinet Office and Detica, a private intel-

25 Soo Hoo, Kevin J. (2000), p. 40.

26 Microsoft, p.71f.

27 Microsoft, p.1.

28 This data is outlined in Microsoft's report, pp 33–77. While the abundance of statistical data may be interesting for industry experts, the report lacks information on counter-strategies and best practices. Notably, qualitative analysis – such as a general portrayal of trends, exemplary cases or development of possible scenarios – are absent from the Microsoft report.

29 Symantec, p.1.

30 PandaLabs, p.19.

31 Sophos, p.50.

ligence solutions company owned by the defense contractor BAE Systems, notes that:

> "Our assessments are, necessarily, based on estimates and assumptions rather than specific examples of cyber-crime, or from data of a classified or commercially-sensitive origin. We have drawn instead on information in the public domain, supplemented by the tremendous knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private-sector organizations".[32]

The report estimates that "the cost of cyber-crime to the UK to be £27bn per annum," and, more specifically, "[a] significant proportion of this cost comes from the theft of IP from UK businesses, which we estimate at £9.2bn per annum."[33] Yet, it not only does not detail how the authors arrived at such figures and but also acknowledges that "the proportion of IP [intellectual property] actually stolen cannot at present be measured with any degree of confidence".[34] Toggling between certainty and ambiguity, the study also claims that "[i]n all probability, and in line with our worst-case scenarios, the real impact of cyber-crime is likely to be much greater".[35] Not surprisingly, the report has been heavily criticized by cybersecurity scholars as being "meaningless",[36] or, as London School of Economics Professor Peter Sommer put it, "[t]he report is full of fake precision." Sommer ultimately calls it an "unfortunate item of British Aerospace puffery"[37] or, in other words, not much more than public relations (PR) for Detica.[38]

1.1.2 Growing Importance of Qualitative Reports

Overall, the critique of surveys that mainly utilize quantitative methods has led to improved threat studies and practices, with qualitative methods gaining more and more weight. In this regard, expert opinions and analysis are used to enhance the more qualitative aspects of cyber threat assessments. Of course, the need for a certain degree of quantitative data remains, but the focus has shifted from relying solely on numbers and statistics to a more general portrayal of trends, analysis of exemplary cases, and the development of future scenarios. Indeed, such efforts offer a good alternative to gathering information about cyber incidents that are either difficult to measure directly, hard to operationalize, or simply difficult to set in a numeric relation. Needless to say, the use of a **mixed-method approach** (that leans more toward qualitative methods) to assess and communicate cyber threats is a trend we observed in this analysis – particularly in the public sector. A striking example is found in the evolution of threat reports by leading Computer Emergency Response Teams (CERTs). The US-CERT, from 2006 to 2009, published "Quarterly Trend and Analysis Reports"[39] containing detailed metrics about cyber threats. It has since stopped publishing these quarterly reports, instead addressing current threats in the "Monthly Activity

32 The Cost of Cybercrime, p.2.

33 Ibid.

34 Ibid, p.16.

35 Ibid.

36 Moore, Tylor. "Why the Cabinet Office's £27bn cyber-crime cost estimate is meaningless," Light Blue Touchpaper, 17 February 2011. Available at: http://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/.

37 Peter Sommer, quoted in: Espiner, Tom. (2011). "Cybercrime cost estimate is 'sales exercise', say experts", ZDNet UK. Available at: http://www.zdnet.co.uk/news/security-threats/2011/02/18/cybercrime-cost-estimate-is-sales-exercise-say-experts-40091866/.

38 This is not to say that industrial IP theft is not a serious threat – the criticism just shows that the attempt at quantifying cyber threats in financial terms may often be problematic and lead to useless and potentially misleading results.

39 US-Cert. (2006). "Quarterly Trends and Analysis Report, 1:1." Available at: http://www.us-cert.gov/press_room/trendsandanalysisQ306.pdf.

Summaries"[40], which is more descriptive. Similarly, from 2002 to 2007, the Australian Computer Emergency Response Team AusCERT conducted yearly "Computer Crime and Security Reviews". However, it has since it stopped such survey work and switched to publishing targeted, specific threat information.[41] The same is true for the Software Engineering Institute's CERT at Carnegie Mellon where from 1995 to 2008 it published detailed vulnerability statistics until it announced: "[W]e are no longer collecting and publishing these statistics [...]".[42] Such examples indicate a shift away from purely quantitative research activity.

As noted, in the private sector quantitative methods continue to play a more prominent role. But, with the exception of Microsoft which relies more on quantitative methods, the other three companies analyzed in this report utilize more of a mixed-method approach. For example, though Symantec lists many figures,[43] the main focus is on *qualitative* analysis. It divides the threats from 2010 into five categories: targeted attacks, social networking and social engineering, zero day exploits, attack kits and mobile threats.[44] Drawing from examples, it provides in-depth descriptions, insight into the trajectory of the threat, and highlights best practices for enterprises and consumers. Of course, Symantec does not refrain from using debatable cost estimates in the report's conclusion, for instance claiming that, "the average cost per incident of a data breach in the United States was 7.2 million".[45] Nevertheless, the report is interesting in the major role that qualitative methods play in assessing and communicating threats and trends. In line with this approach, Sophos and Panda Security also reported some figures but mainly focused on providing detailed descriptions of various reported threats. In fact Sophos alluded to the relevance of this approach stating that:

> "[a]t the root of cybersecurity, it's all about people [...]. Understanding of the threats, the threat methods and the tools we can use to protect ourselves now and in the future is the best and simplest way to minimize the danger".[46]

Indeed, to a certain extent both reports achieve this by providing an overview of the threats and thus raising awareness of the problem.

Returning to the public sector, while we observed that all of the reports favor qualitative methods, the most extensive qualitative analysis of cyber threats is found in the Swiss and the German cases. Interestingly, they resemble the private sector reports produced by Sophos and Panda Security – but, their descriptions of the problems are more detailed and country specific. They also try to avoid framing the threats with exact figures, rather describing them in terms of general, observable trends. This can include: highlighting the spread of new threats, protective measures, and specific qualitative developments.

Overall, the growing utility of qualitative approaches in cyber threat assessments seems understandable given the criticisms of quantitative methods as well as the apparent benefits that come from utilizing a mixed-method approach (i.e. allows reports to speak to tech and non-tech audiences, more in-depth look into key threats, trend analysis, etc.). However, this

40 See, for example: US-CERT. (2009). "Monthly Activity Summary," June. Available at: http://www.us-cert.gov/press_room/monthlysummary200906.pdf.

41 The AusCERT's threat surveys (2002–2006) are available at: http://www.auscert.org.au/render.html?it=2001.

42 See CERT statistics (historical), available at: http://www.cert.org/stats/.

43 Symantec also offers a long version of the same report which can be accessed on http://www.symantec.com/business/threatreport/index.jsp; The long version is similar to the Microsoft (numbers and graphs on most pages) report but it also includes three pages of "best practices" in order to counter threats.

44 Symantec, p.7ff.

45 Symantec, p.17.

46 Sophos, p.48.

observation also presents an opportunity to position this trend within a discussion on the challenges that come with managing today's complex environment – especially for critical infrastructures. For this we now pivot our analysis to the world of complexity science where we characterize cyberspace as a complex system and cyber security (within the CIP domain) as thus a 'complex security challenge' or rather 'complex risk' that requires different tools, concepts, and mindsets in which to manage it.

2. CYBER RISKS AND CRITICAL INFRASTRUCTURES

Though these findings have relevance on their own, they gain even more traction when viewed through the prism of critical infrastructure protection (CIP). Not only since the discovery of Stuxnet – but with far more urgency ever since – has there been a particular focus on the vulnerability of SCADA (supervisory control and data acquisition) systems, or computer systems that monitor and control industrial, infrastructure, or facility-based processes, many of which are considered critical. Through SCADA systems, cyber-incidents can potentially cause severe physical damage in critical infrastructures. Threat assessment in the cyber-domain therefore has a direct link to the broader CIP debate. We first rehash how and why cyberspace is a complex system and what that means for critical infrastructures, before we look at the consequences this has for protection efforts.

2.1. Cyberspace as a Complex System

As is well known, during the 1990s, the rapid growth of the Internet, and broad accessibility of information technology in general, created an entire new sub-layer for virtual interactions and activities to occur between information (technical) networks as well as human (social) networks. Daily activities, such as banking or sending documents between colleagues that were once carried out exclusively in the physical domain, soon met a virtual component. Indeed, in some cases the virtual component has superseded the importance of the physical component or at least operates on the same level of significance. For example, the delivery of many critical services (such as electricity and telecommunications) is now "totally dependent on the Internet and IP-based technology for information and data exchange."[47] In fact, today billions of people are now connected through this borderless virtual playground where individual computers interact with computer networks that control "physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace."[48]

Needless to say, such developments have brought to light the contemporary inter-relationship and dependence between technical, physical and human systems. Such a relationship can be viewed as a large complex system (with systems within systems) that contains many components with varying degrees of connectivity between them. Cyberspace, for instance, is a complex system, "composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables"[49] that is connected to complex critical infrastructures. In fact, the United States Department of Homeland Security (DHS) referred to cyberspace as the "nervous system" of CIs; delivering key public services and goods.[50] Characteristically such systems are non-linear and thus small changes can have big effects. To illustrate, a technical breakdown of a small transformer, caused by the failure in the information network, can cascade into major disruptions across an electrical power grid, manifesting into disruptions to key public services (e.g. electrical power). Comparably, a minor computer glitch in the financial sector can have far-reaching

47 Umberger, Harold and Gheorghe, Adrian, (2011). "Cyber Security: Threat Identification, Risk and Vulnerability Assessment", in: Adrian Gheorghe and Liviu Muresan (eds.), Energy Security: International and Local Issues, Theoretical Perspectives, and Critical Energy Infrastructures. Available at: http://www.springerlink.com/content/p414u4200121012h/fulltext.pdf.

48 US National Strategy to Secure Cyberspace, p.viii.

49 Ibid.

50 Ibid.

economic effects due to human response – such was the case in May 2010 when a computerized sell-off (possibly caused by a simple typing error) triggered the biggest drop ever during a trading day on Wall Street.[51]

In this respect, due to the interacting parts that move between each other at varying speeds, assessing the myriad risks or even trying to anticipate future behavior – as discussed in the previous section – becomes hard to determine and predict. The reason for this is due to the process of emergence, which occurs when the interactions between agents within a complex system self-organize and create novel and coherent structures, patterns and properties. Consequently, finding causal relationships is challenging as new interactions between the agents breed completely new behaviors and phenomena. The following quote from the UK Ministry of Defense captures this tendency:

> "Perhaps the over-riding characteristic of cyberspace is the pace of change. Not just technological change, but changes in business processes and social interactions that this supports; change in impacts that these in turn engender, and vulnerabilities that these expose; and contingent on all of these and on other – non cyberspace – factors the change in threats."[52]

With this in mind, while cyberspace has brought with it many rewards, it has also created a host of new risks, many of which are hard to assess or even see because of the aforementioned complex characteristics. Cyber security thus represents what can be described as 'complex security challenge' or rather 'complex risk' as it is a security issue that becomes difficult to manage due to its characteristics. In other words, the sheer pace of change in the cyber domain (as referenced above) coupled with the changing and broadening scope of cyber threats to public and private organizations makes cyber security an increasingly challenging task. Indeed as Cornish et al. note:

> "Both large and small cyber dependencies and vulnerabilities often go unrecognized in management strategies and risk registers. In some cases cyber risks may be obscured and hidden inside the wider supply chain, several steps removed from the analysis and decision-making centre of a given organization."[53]

Broadly speaking, 'complex risks' – just like complex systems – are characterized by uncertainty (that comes from interactions that breed new behavior and phenomena) coupled with both un/imaginable hazards with un/imaginable consequences. To illustrate this tendency, Cornish et al. interviewed a number of CI operators to examine cyber security issues and stated that "one financial institution reported that the volume and sophistication of [cyber] threats are outstripping the organization's capacity to respond," and that "several organizations reported a significant increase in the threat from insiders."[54] Such interviews revealed that many CI operators were struggling to both understand and manage the cyber intrusions to their systems – in effect their ability to manage the risk was becoming increasingly challenged by the rapidly changing space as well as speed and characteristics of intrusions.

2.2 Consequences of Complexity

System complexity has two immediate consequences for CIP. Charles Perrow's well-known theory claims that technological systems that are interactively complex and tightly coupled will be struck by inevi-

51 Paradis, Tim. "Computer Glitch Haunts Wall Street," The Associated Press, 7 May 2010. Available at: http://www.telegram.com/article/20100507/NEWS/5070561/0/OPINION.

52 UK Ministry of Defense. "Equipment, Support and Technology for UK Defense and Security: A Consultation Paper" (London: The Stationary Office, December 2010, Cm 7989), p.54.

53 Cornish et al (2011), p.6.

54 Ibid.

table accidents. Because of the inherent complexity, independent failures will interact in ways that can neither be foreseen by designers nor comprehended by operators. If the system is also tightly coupled, the failures will rapidly escalate beyond control before anyone understands what is happening and is able to intervene.[55] The very connectedness of critical infrastructures through cyber-means is what poses dangers, because perturbations within them can cascade into major disasters with immense speed and beyond our control.

Further, the dynamic interaction of complex, decentralized, open, unbounded systems amounts to an overtaxing of system managers' abilities to articulate and evaluate them. Complex systems behave contra-intuitively due to parallel occurrences happening at different speeds, irregularities and non-linear cause/effect relationships. The result is that the human brain is unable to "read" these systems correctly; particularly, when we think they work in a simple, causal manner.[56] Unfortunately, analytical frameworks developed for accidents with hazardous materials in the chemical industry and nuclear power plants (risk analysis methodology in the broadest sense) still provide the backdrop for how critical infrastructures (and their cyber-parts) are primarily approached. These traditional risk assessment tools are grounded in strict, measurable assessments and predictive modeling (all of which is based on past behavior and experiences) and linear cause-effect thinking.[57]

Trying to manage complex risks in a dynamic landscape by exclusively utilizing these traditional types of approaches is limiting and can render deceptive results. Again, in reference to the cyber threat reports analyzed in the previous section, one could see the limits of data collection and sampling as well as operationalization of threats as costs. Rather, what is better suited – and arguably needed – to deal with the complex risk posed by cyber threats is **a mixed-method approach**. One that, on the one hand continues to use risk management practices (such as identifying and assessing all known hazards and threats), communicating the risks to concerned bodies (i.e. businesses, broader public, etc.), and implementing prevention and preparation measures that aim at mitigating the likelihood and/or effects of security breaches. But also, on the other hand, appreciates the system's complex characteristics and thus builds up flexibility and adaptability to bounce back from and mitigate the impact of intrusions and security breaches that are bound to occur. This also means building and improving awareness of the *type* of cyber risks that exist in a broad sense. Therefore, on a practical level, publicly available reports should continue to offer if not enhance the role of in-depth analysis and case studies in threat assessments but also, as is now part of so many CIP policies, enhance the *resilience* of a system. Very simply, the less certain we can be about knowing the risks that systems face, the more important the resilience paradigm becomes.

55 Perrow, Charles. "Normal Accidents: Living With High Risk Technologies" (Princeton, NJ: Princeton University Press, 1984).

56 Forrester, Jay. "Industrial Dynamics," (Cambridge, MA: MIT Press, 1961).

57 As a prominent example for this, see: US Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency (Washington DC, 2009), available at: *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*.

3. CONCLUDING ANALYSIS & RECOMMENDATIONS FOR SWITZERLAND

We began this analysis by first looking at the overall similarities and differences of publicly available cyber threat reports – finding that there are some notable differences in approaches to assessing threats that then provided the springboard to examine variance in threat assessment methodology. While quantitative methods have a long history in this area and continue to be a valuable approach to assessing cyber threats, we found that qualitative methods are playing a more prominent role, a trend we see as continuing. This is due to some of the criticism that has been levied against cyber threat assessments, in particular as it relates to data collection and sampling as well as the operationalization of threats as costs. From there, we identified a key trend in cybersecurity assessments that involved using a mixed-method approach that favored qualitative analysis to build awareness and knowledge of cyber threats. Indeed this trend analysis revealed that a majority of the publicly available reports evaluated in the public and private sector increasingly utilize qualitative methodology. Rather than attempting to quantify an ever growing body of viruses, worms and everything else threatening computer systems, cyber threat assessments highlight key trends in attacks/intrusions and protective measures. In some cases, reports will feature in depth case studies – collectively moving in the direction to build situational awareness, encourage cooperation, and knowledge sharing. Finally we attempted to conceptualize this trend within the discussion on managing complex systems and the myriad risks that are born out of such dynamic environments.

For assessing risk in the cybersecurity field, public and private actors in Switzerland use international threat reports, especially those of large cybersecurity companies. Additionally, the Reporting and Analysis Centre for Information Assurance (MELANI) provides information on threats and risks in cyberspace in their semi-annual threat reports (published in collaboration with the Swiss Coordination Unit for Cyber Crime) and issues warnings and advice on current events and trends. The information provided by MELANI often has a specific focus on cases that happened in or are relevant to Switzerland and are therefore a valuable complement to other sources of information for Swiss stakeholders. As mentioned, MELANI does not provide extensive statistical analyses on cyber risks, but outlines specific cases and describes the most relevant or newest threats and risks in more detail. This means that they do not provide an all-encompassing picture on cyber threats, but rather seek to enhance the awareness for specific trends and developments – in effect, improving situational awareness. Yet, one critique of MELANI's approach is that the reports are (at least to a certain degree) confronted with diverging expectations: the broad public (especially the media) wants to get informed about the general level of threats and risks, while the expert community asks for more specific – and also quantitative – information. This tension reveals that a definition of the target audience is at least as important as the selection between more qualitative or more quantitative methodologies for the assessment. Nevertheless, MELANI tries to find a middle ground by providing specific examples that are interesting for both audiences.

To manage contemporary (complex) risks to critical infrastructures, public and private actors in Switzerland should continue to invest in understanding the limits and benefits of comprehensive risk management approaches that draw from **quantitative *and* qualitative methodologies,** the latter of which can help improve what is currently a limited understanding and comprehension of threats and risks in cyber-

space. Within the CI community specifically, apart from a qualitative approach to describe the risks, it also becomes important to provide avenues to share information on risks and effective counter measures through public and private partnerships (PPP) – also beyond the currently established ones. Government actors should encourage CI operators to incorporate cyber security into the broader risk strategy of the organization/company if they have not already done so, as well as ensuring that non-technical staff in CI sectors are engaged in and informed on cyber security measures. All too often, cybersecurity is still seen as mainly a technical issue – which it is not. In addition, PPP meetings can utilize the in-depth analysis and anecdotal evidence of cyber threats in the publicly available reports to further flush out cases that can in turn reinforce cybersecurity awareness for the CI community, namely about the types of security intrusions rather than information on all the threats that have occurred. Such descriptive and analytical assessments enable best practices and lessons learned to be identified – providing signposts for the mitigation of future threats as they manifest. In addition, the *resilience* of information networks and mitigation of cyber threats should be assessed by trying to understand the system's complexity as a whole rather than trying to measure the individual parts. This means that in-depth studies should be performed after cyber threats have manifested and are identified in order to find out how the system was impacted.

None of this is revolutionary or particularly new. In fact, many aspects of current critical infrastructure protection practices already pragmatically deal with the uncertainties of the complex threat environment. There is one important aspect however that has had little reflection. It pertains to how to *communicate* the 'data challenges' in this domain and recognize that experts cannot simply supplement gaps by providing a much desired certainty about the level and development of cyber-threats; and how this influences the ability of governments to provide security. What is lacking is the appreciation that in a world of complex systems, there can be no total security. In fact, the opposite is true: cyber-incidents are deemed to happen, because they simply cannot be avoided. This is a specific challenge for risk communication strategies in the critical infrastructure domain – but also more generally in the security domain.

4.. BIBLIOGRAPHY

The following literature is a list of both articles and reports that we specifically cite in this report as well as additional literature on assessing threats in cyber-security. It is separated into 3 sections: General Literature, Public Sector Reports, and Private Sector Reports.

4.1 General Literature

Baker, Wade H. and Wallace, Linda (2007): "Is Information Security Under Control? Investigating Quality in Information Security Management", Security & Privacy, IEEE 5:1, p. 36–44.

Chuvakin, Anton (2006): "On 2006 CSI/FBI survey". Available at: *http://chuvakin.blogspot.com/2006/07/on-2006-csifbi-survey.html*.

Cornish, Paul et al (2011). "Cyber Security and the UK's Critical National Infrastructure." A Chatham House Report, September 2011. Available at: *http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf*.

CSI (2009) "14th Annual CSI Computer Crime and Security Survey, Comprehensive Edition", Available at: *http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf*.

"Cybersecurity – Assessing Our Vulnerabilities and Developing an Effective Defense, United States Senate Committee on Commerce, Science, and Transportation, One Hundred Eleventh Congress, First Session". March 19, 2009. Available at: *http://www.hsdl.org/?view=docs/testimony/nps37-051109-01.pdf*.

The Economist (2010): A cyber-missile aimed at Iran? 24 September. Available at: *http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm*.

Espiner, Tom (2011): "Cybercrime cost estimate is 'sales exercise', say experts", ZDNet UK. Available at: *http://www.zdnet.co.uk/news/security-threats/2011/02/18/cybercrime-cost-estimate-is-sales-exercise-say-experts-40091866/*.

Forrester, Jay (1961): Industrial Dynamics. Cambridge, MA: MIT Press.

Garretson, Cara and Messmer, Ellen (2006): "It's raining IT security surveys". Network World, Available at *http://www.networkworld.com/news/2006/032006-security-surveys.html*.

Guillot, Alexis and Sue Kennedy (2007): "Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage", Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia. Available at: *http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1026&context=ism&seiredir=1#search=%22Information%20Security%20Surveys%3A%20Review%20Methodologies%2C%20Critics%20Pragmatic%20Approach%20their%20Purposes%20Usage%22*.

Moore, Tyler and Ross Anderson (2011): "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research", Harvard Computer Science Technical Report TR-03-11. Available at: *ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf*.

Moore, Tylor (2011): "Why the Cabinet Office's £27bn cyber-crime cost estimate is meaningless", Available at: *http://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/*.

OECD Global Science Forum (2008): "Applications of Complexity Science for Public Policy: New Tools for Finding Unanticipated Consequences and Unrealized Opportunities", Organisation for Economic Co-operation and Development (OECD), Global Science Forum Report. Available at: *http://www.oecd.org/dataoecd/44/41/43891980.pdf*.

Paradis, Tim (2010): "Computer glitch haunts Wall Street", The Associated Press, 7 May. Available at: *http://www.telegram.com/article/20100507/NEWS/5070561/0/OPINION*.

Perrow, Charles (1984): Normal Accidents: Living With High Risk Technologies. (Princeton, NJ: Princeton University Press, 1984).

Ralston, Patricia A.S. et al. (2007): "Cyber Security Risk Assessment for SCADA and DCS Networks", in: ISA Transactions 46, 583–594.

Soo Hoo, Kevin J. (2000): "How Much Is Enough? A Risk-Management Approach To Computer Security. Consortium for Research on Information Security and Policy (CRISP), Available at *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4127&rep=rep1&type=pdf*.

Suter, Manuel (2006): "Information Security Surveys as Instrument of Risk Analysis", in: ECN European CIIP Newsletter, Volume 2(3), October/November, pp.22–24. Available at: *http://www.irriis.org/ecn/European%20CIIP%20Newsletter%20No%205.pdf*.

Umberger, Harold and Adrian Gheorghe (2011): "Cyber Security: Threat Identification, Risk and Vulnerability Assessment", in Adrian Gheorghe. and Liviu Muresan, (eds.), Energy Security: International and Local Issues, Theoretical Perspectives and Critical Energy Infrastructures, 247–269. Available at: *http://www.springerlink.com/content/p414u4200121ol2h/fulltext.pdf*.

Walsh, Chris (2006): CSI/FBI survey considered harmful. Available at: *http://emergentchaos.com/archives/2006/07/csifbi-survey-considered-harmful.html*.

Winkler, Ira (2006): "Time to end the FBI/CSI study?" Computerworld, 26 September. Available at: *http://www.computerworld.com/s/article/9003640/Time_to_end_the_FBI_CSI_study_*.

4.2 Private sector threat reports

Alperovitch, Dmitri (2011): "Revealed: Operation Shady RAT: An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years." Available at: *http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf*.

Microsoft (2011): "Microsoft Security Intelligence Report Volume 10: An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in 2010". Available at: *http://www.microsoft.com/security/sir/default.aspx*.

Microsoft (2011): "Microsoft Security Intelligence Report. Global Threat Assessments for 117 countries/regions". Available at: *http://www.microsoft.com/security/sir/archive/default.aspx*.

McAfree (2009): "Virtual Criminality Report 2009: Virtually Here: The Age of Cyberwar". Available at: *http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf*

PandaLabs (2010): "Annual Report. Panda Security". Available at: http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf.

Symantec (2011): "Internet Security Threat Report: Trends for 2010". Available at: http://www.symantec.com/business/threatreport/index.jsp.

Symantec (2011): "2011 State of Security Survey: Global Findings". Available at: http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf.

Sophos (2011): "Sophos Security threat report 2011". Available at: http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf.

4.3 Public sector threat reports

AusCERT's threat surveys (2002–2006) are available at: http://www.auscert.org.au/render.html?it=2001

Internet Crime Complaint Center (2010): "Internet Crime Report", National White Collar Crime Center, Bureau of Justice Assistance. Available at: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

Informationssicherung: Lage in der Schweiz und international. Halbjahresbericht 2010/II (Juli – Dezember). MELANI, 2011, Available at: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de&download=NHzLpZeg7t,lnp6IoNTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIF7hGym162epYbg2c_JjKbNoKSn6A--.

Die Lage der IT-Sicherheit in Deutschland 2011. Bundesamt für Sicherheit in der Informationssicherheit, 2011, Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile.

Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK: Jahresbericht 2010. KOBIK, 2011, Available at: http://www.fedpol.admin.ch/content/dam/data/kriminalitaet/internetkriminalitaet/KOBIK/rechenschaftsbericht-2010-de.pdf.

United Kingdom Cabinet Office and Detica (2011): "The Cost of Cybercrime", A Detica Report in Partnership with the Office of Cyber Security And Information Assurance in the Cabinet Office. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

United Kingdom Ministry of Defense (2010): "Equipment, Support and Technology for UK Defense and Security: A Consultation Paper", (London: The Stationary Office, December, Cm 7989).

United States (2003): "The National Strategy to Secure Cyberspace". Available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

United States -Cert (2006): "Quarterly Trends and Analysis Report, 1:1". Available at: http://www.us-cert.gov/press_room/trendsandanalysisQ306.pdf.

United States -CERT (2009): "Monthly Activity Summary, June 2009". Available at: http://www.us-cert.gov/press_room/monthlysummary200906.pdf.

United States Department of Homeland Security (2009): "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency", Washington DC. Available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.