Information & Security: An International Journal

Mchel Rademaker, v.34:2, 2016, 93-104 https://doi.org/10.11610/isij.3407

ASSESSING CYBER SECURITY 2015

Michel RADEMAKER

Abstract: The article is based on the HCSS Report on Assessing Cyber Security.[1] Following the introduction, it identifies fragmentation of reporting and presents threat assessment. Then it highlights the trends in cyber security, followed by a discussion on the importance of developing national cyber strategies. Last but not least, the authors provide general recommendations. The article is based on a review of 70 studies published by public authorities, companies, and research organizations from 15 countries over the last few years, and calls for international efforts to develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments; to systematically anticipate trends and attempt to foresee potential new threats; to develop evidence-based cyber security policies that rely more on data and indicators, rather than subjective perceptions; and to consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.

Keywords: cyber security, strategies, awareness, trends, cyber attacks.

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 of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world (see Figure 1). In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to enhance better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. The Hague Centre for Strategic Studies (HCSS) assessed what is to be known about cyber security threats based on a review of 70 [2] studies published by public authorities, companies, and research organizations from about 15 countries over the last few years (see the bibliography at the end of this article). The questions where: 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?

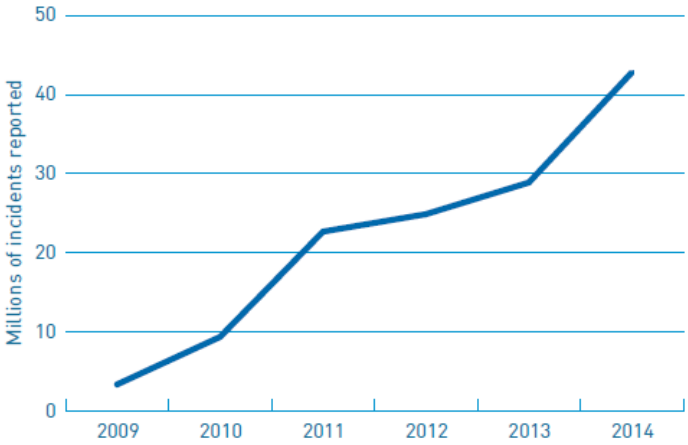

Figure 1: Cyber incidents reported per year (PWC, 2015).

Reporting is Fragmented

The focus of the examined reports differs widely. Some reports look at all possible cyber attacks, while others zoom in on specific threats such as Distributed Denial of Service (DDoS) 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 out of the analysis is that the range of estimates in the examined investigations is so wide, that 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 (Figure 2).

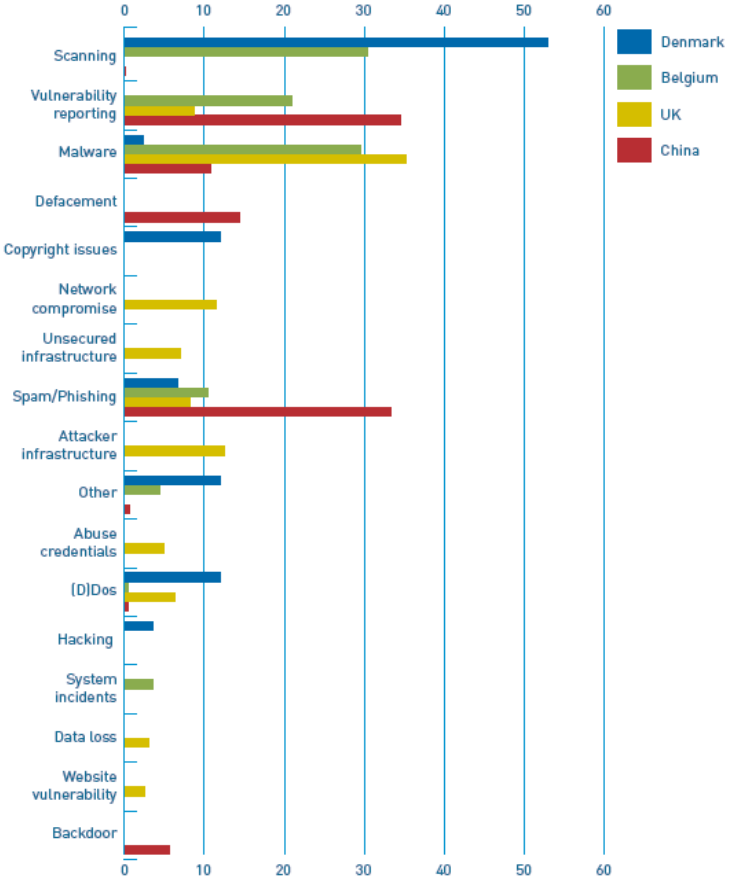

Figure 2: Countries where IP addresses of attack are located (HCSS, 2015).

Trends in Cyber Security

Highlighted are three trends that point to the changing nature of perpetrators. First, a new cyber crime economy is on the rise. An expanding zero-day exploits' market increases the vulnerability of a large share of users. Secondly, 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 (Figure 3).

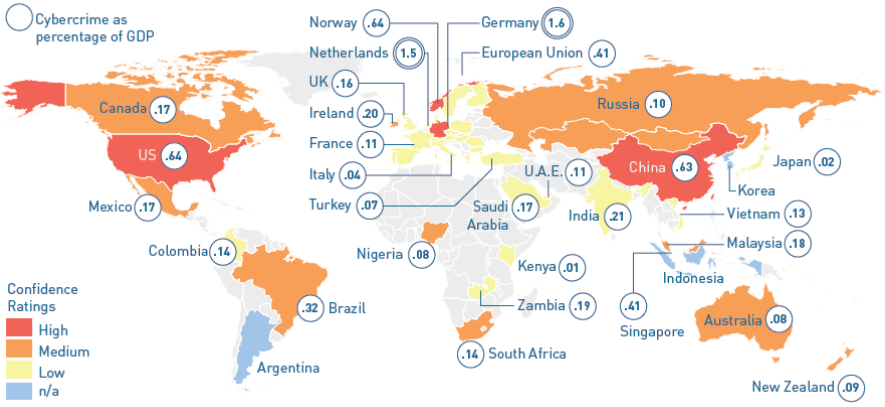

Figure 3: Estimated cost of cyber crime as a percentage of GDP (McAfee, 2015).

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 the rapidly growing spending of cyber security hardware, software and services.

The 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 the 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. To be able to provide a more encompassing and comparable assessment of cyber threats, and create greater awareness thereof, organizations should:

- in line with emerging efforts on the international level, develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments. This will provide more targeted investments in cyber security both on company and government level;
- systematically 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.

Notes:

[1] Erik Frinking and Michel Rademaker, *Assessing Cyber Security* (The Hague: The Netherlands: Hague Centre for Strategic Studies, 16 April 2015), https://hcss.nl/report/assessing-cyber-security.

[2] Maarten Gehem, Artur Ursanov, Erik Frinking, and Michel Rademaker, *Assessing Cyber Security: A Meta-analysis of Threats, Trends and Responses to Cyber Attacks*, Research

report (The Hague, The Netherlands: Hague Centre for Strategic Studies, January 2015), https://www.jstor.org/stable/resrep12567.

Bibliography

"2013 Cyber European Risk Survey," Marsh & McLennan Companies, June 2013, https://www.marsh.com/uk/insights/research/2013-european-cyber-risk-survey.html.

"2013 Data Breach Investigations Report," Verizon, 2013, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

"2013 Global Security Report," Trustwave, 2013, https://www.trustwave.com/Resources/Library/Documents/2013-Trustwave-Global-Security-Report/.

"2014 Data Breach Investigations Report," Verizon, 2014, http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

"2014 Global Report on the Cost of Cyber Crime," Ponemon Insitute, October 2014, https://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime.

"2014 Trustwave Global Security Report," Trustwave, 2014, www.trustwave.com/Resources/Trustwave-Blog/The-2014-Trustwave-Global-Security-Report-Is-Here/.

"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

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

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

"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.

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

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

"Cyber-Attacks: Effects on UK Companies," Centre for the Protection of National Infrastructure and Oxford Economics, July 2014, www.oxfordeconomics.com/my-oxford/projects/276032.

"Cybersecurity: Secure Your Digital Transformation," Capgemini Consulting, 2015, https://www.capgemini.com/resources/cybersecurity-secure-your-digital-transformation/.

"Cybersecuritybeeld Nederland," Nationaal Cyber Security Centrum, October 2014, https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland.

"Cyberspace Operations," Joint Publication 3-12 (R), United States of America, Department of the Army/Department of the Navy, February 2013, https://fas.org/irp/doddir/dod/jp3_12r.pdf.

"D 2.3 List of Current and Future Cyber Security Threats," Capital (Cybersecurity Research Agenda for Privacy and Technology Challenges), June 2014, www.capital-agenda.eu/files/Deliverables/CAPITAL_D2.3_v1.13_submitted.pdf.

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

"De zwakste schakel in de informatiebeveiliging," Utrecht: Capgemini Consulting, September 2013, https://www.capgemini.com/nl-nl/bronnen/de-zwakste-schakel-in-de-informatiebeveiliging/.

"Emerging Cyber Threats Report 2015," Georgia Institute of Technology, Georgia Tech, 2015, https://www.cc.gatech.edu/sites/default/files/images/2015emergingcyberthreatsreport.pdf.

"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.

"ICS-CERT Monitor January-April 2014," National Cybersecurity and Communications Integration Center, 2014, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf.

"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.

"Information Assurance: Situation in Switzerland and Internationally," Semi-annual report 2010/I, Reporting and Analysis Centre for Information Assurance Melani, (January - June), 2014, http://www.news.admin.ch/NSBSubscriber/message/attachments/21041.pdf.

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

"Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015," PriceWaterhouseCoopers, September 2014, www.pwc.lu/en/information-risk-management/docs/pwc-irm-managing-cyber-risks-in-an-interconnected-world.pdf.

"Microsoft Security Intelligence Report," Microsoft Corporations, 2014, https://info.microsoft.com/ww-landing-Security-Intelligence-Report-Vol-23-Landing-Page-eBook.html.

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

"Report on Cyber Security in the Banking Sector," New York State Department of Financial Services, May 2014, https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_banking_report_052014.pdf.

"Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT," Capgemini Consulting and Sogeti High Tech, February 2015, http://www.informeticplus.com/securing-the-internet-of-things-opportunity-putting-cybersecurity-at-the-heart-of-the-iot-capgemini-consulting-y-sogeti.

"State of Risk Report," Trustwave, November 2014, https://www2.trustwave.com/2014-State-of-Risk-Report.html.

"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.

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

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

"Threat Report: H1 2014," F-Secure, April 2014, https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf.

"Trends in Veiligheid 2014," Capgemini Consulting, April 2014, https://www.thehaguesecuritydelta.com/media/com_hsd/report/13/document/Trends-in-Veiligheid-2014.pdf.

"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.

"Websense 2014 Threat Report," Websense, March 2014, www.websense.com/assets/pdf/2014_ThreatReport_Infographic_WEB.pdf.

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, Universita di Roma, December, 2014, https://www.cis.uniroma1.it/media/CIS%20Resources/2014CIS-Report-ENG.pdf.

Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," Intel Security, June 2014, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf.

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

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

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

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

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

Choo, Kim-Kwang Raymond, "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers & Security* 30, no. 8 (November 2011): 719-31, https://doi.org/10.1016/j.cose2011.08.004.

Clapper, James, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 26, 2015, http://fas.org/irp/congress/2015_hr/022615clapper.pdf.

CNCERT/CC, "CNCERT Annual Report 2013," 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," 2014, http://www.brightcloud.com/pdf/CyberEdge-2014-CDR.pdf.

Emm, David, "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.

ENISA, "ENISA Threat Landscape 2013: Overview of Current and Emerging Cyber-Threats," 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.

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

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

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

Federal Financial Institutions Examinations Council, "FFIEC Cybersecurity Assessment: General Observations," 2014, https://www.ffiec.gov/press/pdf/ffiec_cybersecurity_assessment_observations.pdf.

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

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-cy-berthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.

Fortinet, "2014 Threat Landscape Report," 2014, https://bluekarmasecurity.net/wp-content/uploads/2014/10/Fortinet_2014-Threat-Landscape-Report_whitepaper.pdf.

Garnaeva, Maria, Victor Chebyshev, Denis Makrushin, Roman Unuchek, and Anton Ivanov, "Kaspersky Security Bulletin 2014: Overall Statistics for 2014," Kaspersky Lab, 2014. https://securelist.com/kaspersky-security-bulletin-2014-overall-statistics-for-2014/68010/68010/.

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

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, Melissa, "Cyber Readiness Index 1.0," Global Strategies LLC, 2013, http://belfercenter.hks.harvard.edu/files/uploads/Cyber-Readiness-Index-1-0-November-2013.pdf.

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

Luiijf, Eric, Kim Besseling, and Patrick 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* (Oxford, UK, Boston, USA: SOPHOS, 2014), https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf.

Mateski, Mark, Cassandra Trevino, Cynthia Veitch, John Michalski, Mark Harris, Scott Maruoka, and Jason Frye, "Cyber Threat Metrics," Sandia Report, SAND2012-2427, Sandia National Laboratories, March 2012, http://fas.org/irp/eprint/metrics.pdf.

McAfee, "2015 McAfee Labs Threats Report," 2015, https://www.infopoint-security.de/medien/rp-quarterly-threats-nov-2015.pdf.

McAfee, "The Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

Mennen, M.G., ed., "National Risk Assessment 6," Network of Analysis for National Security (ANV), 2014, https://english.nctv.nl/binaries/007328-nrb-6-engels-definitief_tcm32-84267.pdf.

NTT Group, "2014 Global Threat Intelligence Report," 2015, http://www.continuitycentral.com/news07154.html.

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

Robinson, Neil, Luke Gribbon, Veronika Horvath, and Kate Robertson, "Cyber-Security Threat Characterisation," Research Report (Santa Monica, CA: RAND Corporation, 2013, http://www.rand.org/pubs/research_reports/RR235.html.

Shehzad, Ahmad and Torben Sorensen, "TrendRapport," DKCERT, December 2015, https://www.cert.dk/trendrap-port2015/DKCERT_Trendrapport_2015.web.pdf.

United Nations, "The Cyber Index: International Security Trends and Realities," UNIDIR/2013/3 (Geneva, Switzerland: United Nations Institute for Disarmament Research, 2013), http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

Watkins, Bryan, "The Impact of Cyber Attacks on the Private Sector," MindPoint Group, 2014, www.mindpointgroup.com/wp-content/uploads/2014/08/Impact-of-Cyber-Attacks-on-the-Private-Sector.pdf.

About the Author

Michel RADEMAKER is the deputy Director of HCSS. He has fifteen years of hands-on experience as an officer in The Royal Netherlands Army, where he held various military operational and staff posts and also served a term in former Yugoslavia. He has a masters degree obtained at the University of Tilburg. After leaving the armed forces, Mr. Rademaker went on to work at the Netherlands Organisation for Applied Scientific Research (TNO) as a project and program manager and senior policy advisor on security topics for ten years. Eg. as NATO RTO project leader, he and his team developed serious gaming assessment methods and conducted several assessments of security technologies, and worked on numerous strategic security topics.
E-mail: Michelrademaker@hcss.nl.