SEZNAM POUŽITÉ LITERATURY A ZDROJŮ

Ověřeno dne 1. listopadu 2018

ABCLinuxu (2009): Man-in-the-middle. On-line text (http://www.abclinuxu.cz/slovnik/man-in-the-middle).

Abel, R. (2016): Sophisticated nation-state sponsored malware could shut down electric grid. On-line text (https://www.scmagazine.com/nation-state-sponsored-malware-believed-to-target-european-electric-company/article/527878/).

ACLU (2015): FBI equity discussion: Use of Zero days and Policy. On-line verze (https://www.aclu.org/sites/default/files/field_document/zero_days_policy_foia_-_fbi_response.pdf).

Aiken, K. – Horenbeeck, M. (2018): An Internet of Governments: How Policymakers Became Interested in "Cyber". Prezentace na výroční konferenci FIRST, 26. 6. 2018, Kuala Lumpur, Malajsie.

Aishwarya, S. (2011): What is Non-Disclosure Agreement? On-line text (http://blog.ipleaders.in/what-is-non-disclosure-agreement/).

Anderson, R. – Barton, C. – Böhme, R. – Clayton, R. – Eeten, M. J. G. – Levi, M. – Moore, T. – Savage, S. (2012): Measuring the Cost of Cybercrime. In Böhme, R. (ed.): *The Economics of Information Security and Privacy*, pp. 265–300. On-line verze (http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf).

Ball, J. – Borger, J. – Greenwald, G. (2013): Revealed: How US and UK spy agencies defeat internet privacy and security. On-line text (http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security).

Bayuk, J. L. et al. (2012): *Cyber Security Policy Guidebook*. Hoboken: John Wiley.

Best Practice Forum (2014): Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security. On-line text (www.intgovforum.org/cms/documents/ best-practice-forums/establishing-and-supportingcomputer-emergency-response-teams-CSIRTs-for-internetsecurity/409-bpf-2014-outcome-document-computersecurity-incident-response-teams/file).

Boeke, S. – Heinl, C. H. – Veenendaal, M. A. (2015): Civil-Military relations and International Military cooperation in cyber security: common challenges & state practices across Asia and Europe. In Maybaum, M. – Osula, A. M. – Lindström, L. (eds.): *7th International Conference on Cyber Conflict:Architectures in Cyberspace*. Tallinn: NATO CCD COE Publications, pp. 69–80.

Bradshaw, S. (2015): Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. On-line text (https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf).
Britannica (2016): Catch-22. On-line text (https://www.britannica.com/topic/Catch-22-novel-by-Heller).
Brownlee, N. – Guttman, E. (1998): Expectations for Computer Security Incident Response. On-line text (https://www.ietf.org/rfc/rfc2350.txt).
Buchanan, B. – Rid, T. (2015): Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol. 38, No. 1–2, pp. 4–37. On-line verze (http://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382?scroll=top&needAccess=true).
Bunker, R. J. (1996): Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI. On-line text (http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/96autumn/bunker.htm).
Buzan, B. – Wæver, O. – de Wilde, J. (1998): *Security: A New Framework for Analysis.* London: Lynne Rienner Publishers.
Cannell, J. (2013): Tools of the Trade: Exploit Kits. On-line text (https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/).
Cavelty, M. D. (2007): *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* London: Routledge.
Cavelty, M. D. (2012): The Militarisation of Cyber Security as a Source of Global Tension. In Möckli, D. – Wenger, A. (eds.): *Strategic Trends Analysis*, pp. 103–124. On-line verze (http://ssrn.com/abstract=2007043).
CCDCOE (2016a): NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. On-line text (https://ccdcoe.org/nato-recognises-cyberspace--domain-operations-warsaw-summit.html).
CCDCOE (2016b): Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020. Unofficial translation. On-line text (https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf).
CERT/CC (2011): Colombia Case Study. On-line text (http://www.cert.org/incident-management/publications/case-studies/colombia.cfm).
CERT/CC (2015): CSIRT Division Frequently Asked Questions (FAQ). On-line text. (http://www.cert.org/faq/index.cfm#C9).
CERT/CC (2016): CSIRT Services. On-line text (http://www.cert.org/incident--management/services.cfm?).
CERT/CC (2018a): Terms of use. On-line text (https://www.sei.cmu.edu/legal/index.cfm).
CERT/CC (2018b): CSIRT frequently asked questions (FAQ). On-line text (https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf).
CESNET (2018): GÉANT. On-line text (http://archiv.cesnet.cz/provoz/geant.html).
Cormack, A. – Maj, M. – Parker, D. – Stikvoort, D. (2005): CCoP – CSIRT Code of Practice. On-line text (https://www.trusted-introducer.org/CCoPv21.pdf).
CERT Australia (2016): Who we are. On-line text (https://www.cert.gov.au/about).

CSIRT.CZ (2018): Historie. On-line text (https://www.csirt.cz/page/889/historie/).
CSIRT.PL (2015): Raport: Przejęcie domen botnetu Virut. On-line text (https://www.cert.pl/wp-content/uploads/2015/12/Raport_Virut_PL.pdf).
CSTB (1991): *Computers at Risk: Safe Computing in the Information Age*. Washington: National Academy Press.
Daniel, J. – Rychnovská, D. (2015): Mezinárodni politická sociologie: výzkum praxe bezpečnosti. *Mezinárodní vztahy*, No. 1, pp. 26–45.
Daniel, M. (2014): Heartbleed: Understanding When We Disclose Vulnerabilities. On-line text (https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities).
Deibert, R. J. (2002): Circuits of Power: Security in the Internet Environment. In Rosenau, J. N. – Singh, J. P. (eds.): *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany: State University of New York.
Dewar, S. (2017): Active Cyber defense. Zürich: Center for Security Studies (CSS). On-line text (https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/181743/Cyber-Reports-2017-03.pdf?sequence=1).
DoD (2015): The department of defense cyber strategy. On-line verze (http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
Duračinská, Z. (2017): Czech National CSIRT and its role and approach. Prezentace na setkání NatCSIRT, 17. 6. 2017, San Juan.
Duračinská, Z. (2018): Co přináší nová směrnice EU o informační bezpečnosti? On-line text (https://www.systemonline.cz/it-security/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm).
EFF (2011): A Post Mortem on the Iranian DigiNotar Attack. On-line text (https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack).
ENISA (2006): CSIRT cooperation and its further facilitation by relevant stakeholders. On-line text (http://www.enisa.europa.eu/activities/CSIRT/background/coop/files/CSIRT-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport).
ENISA (2007): A basic collection of good practices for running a CSIRT. On-line text (https://www.enisa.europa.eu/publications/a-collection-of-good-practice-for-CSIRT-quality-assurance).
ENISA (2010): Baseline Capabilities of National/Governmental CSIRTs (Part 2 Policy Recommendations). On-line text (https://www.enisa.europa.eu/publications/baseline-capabilities-of-national-governmental-CSIRTs-policy-recommendations/at_download/fullReport).
ENISA (2012a): The Fight against Cybercrime: Cooperation between CSIRTs and Law Enforcement Agencies in the fight against cybercrime. On-line text (https://www.enisa.europa.eu/publications/cooperation-between-CSIRTs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices/at_download/fullReport).

ENISA (2012b): Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. Legal, Regulatory and Operational Factors Affecting CSIRT Co-operation with Other Stakeholders. On-line text (https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing--network-and-information-security-aspects-of-cybercrime/at_download/fullReport).

ENISA (2013): CSIRT community: Recognition mechanisms and schemes. On-line text (https://www.enisa.europa.eu/publications/CSIRT-community-recognition--mechanisms-and-schemes/at_download/fullReport).

ENISA (2015): Information sharing and common taxonomies between CSIRTs and Law Enforcement. On-line text (https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law--enforcement/at_download/fullReport).

ENISA (2017): Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects. On-line text (https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement/at_download/fullReport).

ENISA (2018a): CSIRTs Network. On-line text (https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network).

ENISA (2018b): CSIRTs by Country – Interactive Map. On-line text (https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/CSIRTs-by-country--interactive-map).

ERCT (2013): Environmental Risks: Cyber Security and Critical Industries. Environmental Cyber Risk Whitepaper. On-line text (https://www.xlcatlin.com/~/media/fff/pdfs/environmental_cyber-risks_whitepaper_xl.pdf).

EU (2016): Směrnice evropského parlamentu a rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV. On-line verze (http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32013L0040&qid=1479131762910&from=EN).

Fidler, M. (2015): Regulating the zero-day vulnerability trade: a preliminary analysis. On-line text (http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf).

FIRST (2018a): FIRST History. On-line text (https://www.first.org/about/history).

FIRST (2018b): FIRST Vision and Mission Statement. On-line text (https://www.first.org/about/mission).

FIRST (2018c): What are the benefits of FIRST? On-line text (https://www.first.org/membership/benefits).

Fogleman, R. R. (1995): Information Operations: The Fifth Dimension of Warfare. Remarks as delivered by Gen. Ronald R. Fogleman. On-line text (http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm).

Fox, D. G. (2013): Solving The Cybersecurity Puzzle. On-line text (https://www.pgjonline.com/2013/02/05/solving-the-cybersecurity-puzzle/).

Frei, S. (2013): The Known Unknowns: Empirical Analysis of Publicly Known Security Vulnerabilities. On-line text (http://www.techzoom.net/Papers/The_Known_Unknowns_(2013).pdf).

Friedman, A. – Singer, W. P. (2014): *Cybersecurity and Cyberwar. What Everyone Needs to Know.* New York: Oxford University Press.

GÉANT (2016a): GÉANT. About our membership. On-line text (http://www.geant.org/About/Membership).

GÉANT (2016b): Processes: Accreditation. On-line text (https://www.trusted--introducer.org/processes/accreditation.html).

Gheorghe, A. (2014): What Is End-to-End Encryption? Why Should You Care. On-line text (https://hotforsecurity.bitdefender.com/blog/what-is-end-to-end--encryption-why-should-you-care-10952.html).

Gonzales, J. J. – Kossakowski K. P. – Wiik, J. (2005): Limits to Effectiveness in Computer Security Incident Response Teams. On-line text (https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_53057.pdf).

GovCERT.CZ (2016): Co je NCKB. On-line text (https://www.GovCERT.CZ/cs/).

GOV-CERT.RU (2016): Информация о GOV-CERT.RU. On-line text (http://www.gov-cert.ru).

Guardian (2018): The NSA files. On-line text (https://www.theguardian.com/us--news/the-nsa-files).

Hall, P. A. (1986): *Governing the Economy: The Politics of State Intervention in Britain and France.* New York: Oxford University Press.

Haler, J. – Merrell, S. A. – Butkovic, M. J. – Willke, B. J. (2011): Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability. On-line text (www.sei.cmu.edu/reports/11tr015.pdf).

Hansen, L. – Nissenbaum, H. (2009): Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, Vol. 53, pp. 1155–1175.

Harris, S. (2013): *CISSP All-In-One Exam Guide.* Columbus: McGraw-Hill.

Hník, V. et al. (2012): Vývoj související s budováním pracovišť typu CERT/CSIRT v České republice. *Ochrana & Bezpečnost*, roč I, č. 3. On-line verze (http://ochab.ezin.cz/O-a-B_2012_C/2012_C_09_nemeckova.pdf).

Holtfreter, K. – Meyers, T. J. (2015): Challenges for Cybercrime Theory, Research, and Policy. In Lajeunesse, G. C. (ed.): *The Norwich Review of International and Transnational. The 2015 Inaugural Edition.* On-line verze (https://static1.squarespace.com/static/516ffcf4e4b06eef9180b5bd/t/5627aee0e4b01ab7af225a1d/1445441248430/NRITCPub.pdf#page=62).

Horsley, Ch. (2014): New Zealand National CSIRT Establishment: CSIRT Profiles and Case Studies. On-line text (https://internetnz.nz/sites/default/files/submissions/New_Zealand_National_CSIRT_Profiles.pdf).

Howard, D. J. (1997): An Analysis of Security Incidents on the Internet 1989–1995. On-line text (http://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf).

Husák, M. (2012): Monitorování síťového provozu honeypotu. Diplomová práce. Brno: Masarykova Univerzita.
Chander, A. – Uyen, L. (2014): *Breaking the Web: the Global Internet v/s Data Localization*. UC Davis Legal Studies Research Paper Series Research Paper No. 378. On-line verze (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858).
Chander, A. – Uyen, L. (2015): Data Nationalism. *Emory Law Journal*, Vol. 64, No. 3, pp. 677–739.
Choucri, N. – Madnick, S. – Ferwerda, J. (2014): Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, Vol. 20, No. 2, pp. 96–121. On-line verze (http://dx.doi.org/10.1080/02681102.2013.836699).
Choucri, N. – Madnick, S. – Koepke, P. (2016): Institutions for Cyber Security: International Responses and Data Sharing Initiatives. On-line text (http://web.mit.edu/smadnick/www/wp/2016-10.pdf).
IGF (2014): BPF3 – Establishing and Supporting CSIRTs for Internet Security. On-line video (https://m.youtube.com/watch?v=YnOljPgfqmI).
Ihned.cz (2008): Armáda převezme všech 15 vozů Dingo 2 do konce měsíce. On-line text (https://domaci.ihned.cz/c1-30022840-armada-prevezme-vsech-15-vozu-dingo-2-do-konce-mesice).
Ihned.cz (2017): Výdaje kybernetického úřadu NÚKIB se letos vyšplhají na 214 milionů Kč. On-line text (https://ictrevue.ihned.cz/c3-65667140-0ICT00_d-65667140-vydaje-kybernetickeho-uradu-nukib-se-letos-vysplhaji-na-214-milionu-kc).
ITU (2016): Introduction to Computer Security Incident response Team (CSIRT). On-line text (http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Session%202%20-1115-1230-v09-10-2016.pdf).
Jaroszewski, P. (2017): On a bumpy road towards Polish National Cybersecurity Center. Prezentace na setkání NatCSIRT, 17. 6. 2017, San Juan.
Jirásek, P. – Novák, L. – Požár, J. (2015): *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie České republiky.
Jontz, S. (2016): U.S. Army Creates Cybersecurity Strategy For a New Normal. On-line text (http://www.afcea.org/content/?q=Article-us-army-creates-cybersecurity-strategy-new-normal).
Kallberg, J. – Thuraisingham, B. (2013): Cyber Operations. Bridging from Concept to Cyber Superiority. *Joint Forces Quarterly*, 1st quarter 2013, No. 68, pp. 53–58. On-line verze (http://cyberdefense.com/files/JFQ-68_53-58_Kallberg-Thuraisingham.pdf).
Kaskina, B. (2017): CSIRT collaboration in Europe. Prezentace na EUNITY Project Workshop, 11.–12. říjen 2017, Japonsko. On-line prezentace (http://eunity-project.eu/m/filer_public/9d/34/9d348d5b-47e2-42d4-a330-ce7b4bf3c331/baiba_kaskina_csirts-europe-v21.pdf).

Killcrece, G. (2004): Steps for creating national CSIRTs. On-line text (http://www.CSIRT.org/archive/pdf/NationalCSIRTs.pdf).
Killcrece, G. – Kossakowski, K. P. – Ruefle, R. (2003): State of the Practice of Computer Security Incident Response Teams (CSIRTs). On-line text (ftp://192.58.107.24/public/documents/03.reports/pdf/03tr001.pdf).
Kropáčová, A. (2018): Nesmíme se nechat zahltit zákony, říká šéfka nejstaršího českého CSIRT týmu. Rozhovor s Andreou Kropáčovou. On-line text (https://www.root.cz/clanky/nesmime-se-nechat-zahltit-zakony-rika-sefka-nejstarsiho-ceskeho-csirt-tymu).
Kumar, S. M. V. (2010): Are joint ventures positive sum games? The relative effects of cooperative and noncooperative behavior. *Strategic Management Journal*, No. 32, pp. 32–54. On-line verze (http://www.sawislibrary.co.za/dbtextimages/62590.pdf).
Layden, J. (2013): Spyware Virus Stealing Indian Government/Military Info Found on U.S.-Based Computer Server. On-line text (http://www.matthewaid.com/post/57703467720/spyware-virus-stealing-indian-governmentmilitary).
Leiner, B. M. et al. (1997): The past and future history of the Internet. *Communications of the ACM*, Vol. 40, No. 20. On-line verze (http://bnrg.eecs.berkeley.edu/~randy/Courses/CS294.S13/1.1x.pdf).
Lewis, K. A. – Timlin, K. (2011): Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. On-line text (http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf).
Libicki, M. C. (2009): Cyberdeterrence and Cyberwar. On-line text (http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf).
Longstaff, T. A. et al. (1997): Security of the Internet. On-line text (http://resources.sei.cmu.edu/asset_files/SpecialReport/1996_003_001_496597.pdf).
Lowe, C. R. (2005): Commercialisation and Spin-Out Activities of the Institute of Biotechnology. *Journal of Commercial Biotechnology*, Vol. 11, No. 4, pp. 206–317. On-line verze (http://dx.doi.org/10.1057/palgrave.jcb.3040131).
Luiijf, E. – Healey, J. (2012): Organisational structures & considerations. In Klimburg, A. (ed.): *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication.
Madnick, S. – Li, X. – Choucri, N. (2009): *Experiences and Challenges with Using CSIRT Data to analyze*. Massachusetts Institute of Technology Engineering Systems Division Working Paper Series. On-line verze (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478206).
Microsoft (2018): What is middleware? On-line text (https://azure.microsoft.com/en-us/overview/what-is-middleware/).
Mishra, N. (2016): Data localization laws in a digital world: Data protection or data protectionism? On-line verze (http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf).

Morgus, R. (2015): The FBI Should Stop Undermining Norms Before They Take Root. On-line text (https://www.justsecurity.org/28343/fbi-stop-undermining--norms-root/).
NATO (2014): Wales Summit Declaration. On-line text. (http://www.nato.int/cps/en/natohq/official_texts_112964.htm).
NCSC-NL (2016): Taranis. On-line text (https://www.ncsc.nl/english/Incident+Response/monitoring/taranis.html).
Nielsen, N. (2017): EU seeks to decrypt messages in new anti-terror plan. On-line text (https://euobserver.com/justice/139524).
Nissenbaum, H. (2005): Where Computer Security Meets National Security. *Ethics and Information Technology*, Vol. 7, No. 2, pp. 61–73.
NSKB (2015): Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. On-line verze (https://www.GovCERT.CZ/download/nodeid-1004/).
Obama, B. (2009): Remarks by the President on Securing Our Nation's Cyber Infrastructure, 29 May 2009. On-line text (https://www.whitehouse.gov/the--press-office/remarks-president-securing-our-nations-cyber-infrastructure).
OECD (2005): The promotion of a culture of security for information systems and networks in OECD countries. On-line text (http://www.oecd.org/internet/ieconomy/35884541.pdf).
OECD (2012): A Secure Internet as an Engine of Economic Growth. On-line text (http://www.oecd.org/internet/asecureinternetasanengineofeconomic-growth.htm).
OWASP (2015): Man-in-the-middle attack. On-line text (https://www.owasp.org/index.php/Man-in-the-middle_attack).
Pačka, R. (2017): *Role národních Computer Emergency Response Teams (CERT) v zajišťování kybernetické bezpečnosti státem*. Rigorózní práce. Brno: FSS MU.
Peretti, K. – Slade, J. (2014): State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction. Cyber alert: A Publication of the Security Incident Management & Response Team. On-line verze (http://www.alston.com/files/Publication/0470bf82-1589-4200-be02-de03a3aea95b/Presentation/PublicationAttachment/35553890-a8a6-4eb5-b7bf-e6397539d409/14-183-State--Sponsored-Cybercrime.pdf).
Perez, T. – Segalis, B. – Navetta, D. (2015): Energy cybersecurity – a critical concern for the nation. On-line text (http://www.dataprotectionreport.com/2015/04/energy-cybersecurity-a-critical-concern-for-the-nation/).
Perlroth, N. (2014): Experts Find a Door Ajar in an Internet Security Method Thought Safe. On-line text (http://bits.blogs.nytimes.com/2014/04/08/flaw--found-in-key-method-for-protecting-data-on-the-internet/).
Perlroth, N. – Sanger, D. E. (2013): Nations Buying as Hackers Sell Flaws in Computer Code. On-line text (http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html).

Peters, B. G. (1996): Political Institutions, Old and New. In Goodin R. E. – Klingemann H. D. (eds.): *A New Handbook of Political Science*. New York: Oxford University Press, pp. 205–220.

Purpura, P. (2007): *Security and Loss Prevention: An Introduction*. San Diego: Butterworth-Heinemann.

Ruefle, R. – Dorofee, A. – Mundie, D. – Householder, A. D. – Murray, M. – Perl, S. J. (2014): Computer Security Incident Response Team Development and Education. *IEEE Security & Privacy*, Vol. 12, Issue 5, pp. 16–26.

Russell, A. L. (2014): *Cyber Blockades*. Washington: Georgetown University Press.

Seclist.us (2017): IntelMQ is a solution for it security teams for collecting and processing security feeds using a message queuing protocols. On-line text (http://seclist.us/intelmq-is-a-solution-for-it-security-teams-for-collecting-and--processing-security-feeds-using-a-message-queuing-protocols.html).

Sharma, A. (2009): Cyber wars: a paradigm shift from means to ends. In Czosseck, C. – Geers, K. (eds.): *The virtual battlefield: perspectives on cyber-warfare*. Amsterdam: IOS Press, pp. 3–17.

Schneier, B. (2014): Regin: Another Military-Grade Malware. On-line text (https://www.schneier.com/blog/archives/2014/11/regin_another_m.html).

Schneier, B. (2016): The value of encryption. On-line text (https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html).

Skierka, I. – Morgus, R. – Hohmann, M. – Maurer, T. (2015a): CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams. Working paper. On-line verze (http://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf).

Skierka, I. – Morgus, R. – Hohmann, M. – Maurer, T. (2015b): National CSIRTs and Their Role in Computer Security Incident Response. On-line verze (http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf).

Slížek, D. (2014): Heartbleed Bug: jak se k chybě v OpenSSL staví české i světové firmy. On-line text (http://www.lupa.cz/clanky/heartbleed-bug-jak-se-k-chybe-v--openssl-stavi-ceske-i-svetove-firmy/).

Speser, P. (2008): *What Every Researcher Needs to Know About Commercialization*. Providence: Foresight Science & Technology Inc.

Štědroň, B. (2009): *Open Source software ve veřejné správě a soukromém sektoru*. Praha: Grada.

Tahvanainen, A. – Nikulainen, T. (2011): Commercialisation at Finnish Universities: Researchers' Perspectives on the Motives and Challenges of Turning Science into Business. In Discussion Paper 1234. Helsinki: The Research Institute of the Finnish Economy. On-line verze (https://www.etla.fi/wp-content/uploads/2012/09/dp1234.pdf).

Tkachuck, N. (2016): Countering cyber threats to national security: Ukraine defends its cyber infrastructure in the face of attacks from Russia. *Per Concordiam: Journal of European Security and Defense Issues*, Vol. 7, Issue 2, pp. 52–56.
Traynor, I. (2007): Russia accused of unleashing cyberwar to disable Estonia. On-line text (https://www.theguardian.com/world/2007/may/17/topstories3.russia).
UN (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. On-line verze (http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
UNODC (2013): Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. On-line text (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf).
USSC (2015): U.S. Cyber Command factsheet. On-line text (https://www.stratcom.mil/factsheets/2/Cyber_Command/).
Verizon (2015): 2015 Data Breach Investigations Report. On-line text (https://msisac.cisecurity.org/whitepaper/documents/1.pdf).
VS (2017): Medzinárodná akreditácia útvaru CSIRT.MIL.SK. On-line text (http://vs.mosr.sk/medzinarodna-akreditacia-utvaru-csirt-mil-sk/).
Wæver, O. (1995): Securitization and Desecuritization. In Lipschutz, R. D. (ed.): *On Security*. New York: Columbia University Press, pp. 46–86.
Weimann, G. (2004): Cyberterrorism. How Real Is the Threat? Special Report 119. United States Institute of Peace. On-line verze (https://www.usip.org/sites/default/files/sr119.pdf).
Weinstein, J. M. – Drake, W. L. – Silverman, N. P. (2015): Privacy vs. Public safety: Prosecuting and defending criminal cases in the post-snowden era. *American Criminal Law Review*, Vol. 52. On-line verze (http://www.steptoe.com/assets/htmldocuments/2015%20Featured%20Article.PDF).
Welch, L. D. (2011): Cyberspace – the fifth operational domain. On-line text (https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf).
West-Brown, J. M. – Stikvoort, D. – Kossakowski, K. P. – Killcrece, G. – Ruefle, R. – Zajicek, M. (2003): *Handbook for Computer Security Incident Response Teams (CSIRTs)*. 2nd edition. On-line verze (http://www.sei.cmu.edu/reports/03hb002.pdf).
White House (2011): International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World. On-line verze. (https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).
Wueest, C. (2014): Targeted Attacks Against the Energy Sector. On-line text (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf).
Yould, R. E. (2003): Beyond the American Fortress: Understanding Homeland Security in the Information Age. In Latham, R. (ed.): *Bombs and Bandwidth:*

The Emerging Relationship Between Information Technology and Security. New York: The New Press, pp. 74–98.
Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. On-line verze (https://portal.gov.cz/app/zakony/download?idBiblio=47807&nr=106~2F1999~20Sb.&ft=pdf).
Zetter, K (2015): Turns Out the US Launched Its Zero-Day Policy in Feb 2010. On-line text (https://www.wired.com/2015/06/turns-us-launched-zero-day--policy-feb-2010/).
Zetter, K. (2016): Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. On-line text (https://www.wired.com/2016/03/inside-cunning--unprecedented-hack-ukraines-power-grid/).
ZSKB (2018): Zpráva o stavu kybernetické bezpečnosti za rok 2017. On-line text (https://www.govcert.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf).