

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Hytönen, E. ; Trent, A. & Ruoslahti, H. (2022) Societal Impacts of Cyber Security in Academic Literature: Systematic Literature Review. In Thaddeus Eze, Nabeel Khan and Cyril Onwubiko (Eds.) Proceedings of the 21st European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited, 86-93.

doi: 10.34190/eccws.21.1.288

Available at: <https://doi.org/10.34190/eccws.21.1.288>

[CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)

Societal Impacts of Cyber Security in Academic Literature: Systematic Literature Review

Eveliina Hytönen, Amir Trent and Harri Ruoslahti¹

Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland

Eveliina.Hytonen@laurea.fi

Harri.Ruoslahti@laurea.fi

Abstract: The 2020 Allianz Risk Barometer, with 39% of responses, ranked cyber incidents as the number one risk threatening business continuity. Any organisation may face a number of challenges e.g. costly data breaches, ransomware incidents, and even litigation after an event. The Internet has, in many ways, changed society, transformed businesses, organisational communication and learning. People can now interact through social networking platforms. Modern society has become very technology driven, as ICT is now an integral component in peoples' lives. However, besides the many benefits that the Internet and other ICT technology bring, there are also threats, such as cyber-attacks looking to exploit vulnerabilities in ICT applications and systems. This study is a systematic literature review that explores how societal impacts of cyber security in modern society are discussed in academic literature. The Introduction discusses the overall importance of cyber security in today's society. The body of this paper presents the method in which the literature review was conducted, and a concise summary of the findings that answer the research question: How are societal impacts of cyber security discussed in academic literature? Six categories of investigation of societal impacts of cyber security are identified: 1) Impacts on Social and Societal Levels, 2) Detection of cyber-crime and incidents, 3) Critical infrastructures and services, 4) Impacts of incidents and individual technology, 5) Cybersecurity awareness, and 6) Cybersecurity and collaboration. Lastly, the conclusions, based on the research findings, address the feasibility, impact, strengths, weaknesses and possible ethical concerns of cybersecurity. This paper contributes to the overall understanding of current societal impacts of cyber security, and this understanding benefits the development of methods that assess societal impacts, as well as provides focus for future training and development of cyber and e-skills needed for better awareness of cyber threats, and to better address possible cyber incidents.

Keywords: society, cyber security, societal impacts


1. Introduction

In 2020, cyber incidents ranked as the most important business risk in the Allianz Risk Barometer (2020). Thus, businesses face a number of challenges such as large and costly data breaches, ransomware incidents and increasingly the prospect of litigation after an event. In 2013 cyber incidents had finished 15th, driven by companies' increasing reliance on data and IT systems, awareness of cyber threats have grown very quickly.

The Internet has changed many aspects of society, as it has transformed businesses, organisational learning, as it has enabled interaction between people through social networking platforms, so due to the emergence of the Internet, today's society today has evolved into a technological driven world (Chamie, 2020). ICT has essentially become an integral component to peoples' everyday lives, and besides the many benefits of the Internet and other ICT technology, there are unfortunately also threats, such as cyber attackers with malicious intent, who look to exploit vulnerabilities within these ICT applications (Singh, 2012).

Cyber risks continue to evolve, in e.g. significant increases in the numbers of ransomware incidents drive up the frequency of losses for companies. Overall, cyber-attacks are becoming more sophisticated and targeted as criminals seek higher rewards with multimillion-dollar extortion demands (Allianz Risk Barometer, 2020). Singh (2012) finds that e-skills are essential, due to the influence that ICT has on society, its organisations, and members, so investing in ICT skills provide needed possibilities to build competences to protect against cyber threats.

The purpose of this literature review is to identify how societal impacts of cyber security, and how the impacts of cyber security issues to individuals, communities, organizations or societies are discussed in academic literature. The goal of project ECHO (European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations) is to organize a networked approach that by effective and efficient multi-sector collaboration aims at strengthening proactive cyber security in the European Union. The project ranges from 2019 to 2023 (ECHO, 2020; Yanakiev, 2020). This study adds in part to the practical body of knowledge that the

¹  <https://orcid.org/0000-0001-9726-7956>

project cumulates, while also extending current theoretical knowledge regarding the impacts that cyber security may have on society. The research question of this study is: How are societal impacts of cyber security discussed in academic literature?

2. Methodology

The method used in this research is a systematic literature review. This is a qualitative study. Systematic literature reviews are useful in identifying knowledge gaps in current literature, and bring new insights to the respective field for further investigation (Kitchenham, 2004).

2.1 Qualitative research design

According to Kitchenham (2004), a systematic literature review is a through process that can help present evidence that showcases the effects of selected events as they are described in research literature, and which may not be conveyed in traditional non-systematic literature reviews. Systematic literature reviews may thus, be more extensive than traditional ones. To conduct this literature review an academic search was conducted to provide answers to the research question. This study was conducted in a series of four steps: 1) search, 2) inclusion criteria, 3) DET analysis, and 4) writing of results and conclusions.

2.2 Search, inclusion criteria and DET-analysis

The search for the articles was performed in April 2020. The search was conducted using the Google Scholar, where a Boolean keyword search with the combination of “societal impacts of cyber-security + ICT + security + society + impact” were used as search parameters. The period for the search spanned literature published within the six-year period of 2014 - 2020.

The initial Google Scholar search returned a total of 265 peer reviewed articles. The abstract of these articles were examined against inclusion criteria: societal impact and cyber security keywords included in abstract, title and subject terms, Full Text and relevant to Research Question. The final sample included 33 papers that correspond to the inclusion criteria.

Following the identification of the appropriate peer reviewed articles for the literature review all 33 articles were read, and analysed by extracting relevant pieces of information to a data extraction table (DET) that was based on the research question. The next chapter of this paper discusses the findings of the sample articles.

3. Findings

Six streams of academic discussion emerge from the data. 1) Eleven papers discuss Impacts on social and societal levels, 2) four paper focus on Detection of cyber-crime and incidents, 3) seven papers relate to impacts on critical infrastructures, 4) five papers relate to impacts of individual incidents and technology, 5) seven papers discuss awareness building and training, 6) two papers look at creating common understanding of cyber security.

3.1 Impacts on social and societal levels

Eleven papers discuss Impacts on social and societal levels.

Schia and Gjesvik (2018) take a broader approach to cyber security than just national security, as they consider wider economical and societal impacts of digitization. 1) Cyber security has impacts on states and stakeholders. Digital technologies can promote freedom, as they provide digital arenas for expression of thought and debate free from governmental constraints; 2) Strengthen cyber security on an international level, because security on the online arena is only as strong as its weakest link, so focus on improving developing states to improve global cybersecurity structures; 3) Importance of digitalization and ICT in fostering economic and societal development is increasing, and there is a need to protect these benefits by cyber security.

Michel and King (2019) find that the Internet and connected technology platforms have enabled an increase of cyber influence and actions ranging from personal to national level security. Understanding how awareness (e.g. understanding what is real vs. fake) effects human decisions, may help avoid falling prey to cybercriminals cyber influence, and Internet fraud; appropriate technology can aid to increase cyber awareness by providing detection and support.

Kallberg & Burk (2014) promote defending national infrastructure from cyberattacks to protect information, network availability, and the global information grid, and to safeguard the lives of its citizens, protect their property, and preserve needed ecosystems and the ecosystem services. Attacks may cause environmental damages and have impact on societal stability.

Glisson and Choo (2017) find that the continued and increasing fusion of technology into wider dimensions of everyday life encourages cyber-crime. Hence, promoting evolution and diversification of cybersecurity, and responses that address growing concerns to highlight, investigate and address cyber-security vulnerabilities, especially in the context of cyber-of-things, the changing landscape demonstrates a need to develop innovative managerial, technological and strategic solutions.

La Torre, Dumay and Rea (2018) note that there is great societal power in Big Data. Stemming from cyber threats, the authors identify a need for corporate accountability, and call for a human-oriented approach to by understanding what detrimental implications the increasing usage of big data has for businesses and society, to promote equal society, transparency and a better decision-making big data. According to Bradshaw (2018) society is mostly aware of emerging technologies, and study to understand the impacts of novel innovations on society and the lives of its members is needed. Increased governmental oversight may be needed, and policy makers should prepare for a technology-driven disruption of society.

Afonasova et al. (2019) have studied the ways in which socio-economic background can affect how to allocate conditions for a transition to the digital economy. The authors find that focus should be put on management, information infrastructure, research and development, human resources and education, information security, smart city technology, and digital healthcare to boost to digitalization.

3.2 Detection of cyber-crime and incidents

Four paper focus on Detection of cyber-crime and incidents.

Gañán, Ciere and van Eeten (2017) find that cybercrime impacts are not limited to the direct consequences of a cyber-attack, but that there are significant costs to the well-functioning of the economy. The authors propose effective economic impact assessment with systematic data collection, guided by identified factors and indicators.

Tarafdar, Gupta, and Turel (2015) focus on, what they call the 'dark side' of information technology (IT) use. They find that cybercrime and other illicit use of information and communications technology (ICT) can seriously infringe the wellbeing of individuals, organizations, and society. Ibrahim et al. (2019) find that cyber-attacks have many impacts on national security, even putting the political, economic, and social welfare of the state in jeopardy, so a cyber warfare challenge on a national level, is rapidly detecting relevant threats as the scale of potential damages can be substantial if e.g. critical services are attacked.

Cuquet et al. (2017) see that data-driven innovations and business models, and data analytics of big data can improve event detection, situational awareness, and decision-making, and efficient allocation of resources; Interoperability is a key enabling factor, as is including data skills to general educational programs, and updating of legal frameworks to promote positive big data practices that positively address societal concerns.

3.3 Critical infrastructures and services

Seven papers relate to impacts on critical infrastructures.

Rajaonah (2017) notes that few studies on information systems combine trust and security, and those that do are mostly limited to two-agent interactions. The authors propose to introduce more holistic approaches of critical infrastructure protection (CIP), as information systems and the Internet are at the core of most modern businesses and services, and the information and knowledge stored and exchanged are of great value, which can attract cyber-attacks on information systems that can directly affect vital services; Critical infrastructures involve vital services, and their disruption have a significant impact on vital functions of society, so protecting society from cyber-attacks and ensuring people's well-being becomes a government level concern.

McLeod and Dolezel (2018) note unprecedented rates of health care data breaches. Elements associated with data breaches can be considered as: organizational factors, business process exposure factors, and technological security factors; Understanding these factors, and using computer security industry frameworks and healthcare standards, may help predict healthcare data breach weaknesses.

Steiger et al. (2018) propose that it is crucial to discuss hypothetical scenarios and analyse actual events, to achieve better understanding of cyber conflicts, and also: 1) Besides Western sources, also work with e.g. Russian and Chinese speaking coders; 2) Recognise the attribution made by actual conflict actors; 3) Rely on structured inclusion criteria to establish a dataset to evaluate cyber incidents; and 4) Build assessments on transparent indicators and develop criteria to gauge the intensity of cyberattacks that may represent the severity of cyber incidents.

Touhiduzzaman et al. (2019) view risk assessment important in understanding the potential consequences related to critical infrastructure. Different risk assessment methods vary in their goals, application domains, impacts, and consequences, and selection of appropriate method of risk assessment can be made based on the advantages and disadvantages associated with each respective method.

Rajamäki and Knuutila (2015) show that public protection and disaster relief may form a complex software-intensive system that consists of several different sub-systems (e.g. 112-services, law enforcement, emergency medical services, firefighting and rescue services), which may be divided into many sub-sub-systems, calling for: 1) Proactive models of information security driven by awareness of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries; 2) Effective tools and methods help cope with challenges of dynamic risk landscape with self-healing; 3) Integrate cyber security to every-day life, where efficient usage of tools and methods enable stakeholders co-operate, while protecting their privacy, and creating heightened public awareness and understanding.

Kotzanikolaou, Theoharidou and Gritzalis (2013) note the need to focus on assessing risks caused by the multi-order dependencies of critical infrastructures, and to resolve some major challenges: data accessibility, model development, model validation, and access to reliable real-time data to identify failures related dependencies. Methodologies should examine how threats and their impact may transfer from one infrastructure to another by identifying dependencies that may be based on existing security plans and service level agreements.

Adlakha et al. (2019) find that unawareness among the masses is surprisingly common, and while organizations need to maintain their security goals that in order to prevent the attacks, people should be aware that the more technology they use, the more vulnerable they become to possible attacks; Cyber criminals use evolving measures to get their hands on confidential information, and most cyber-attacks could be avoided by employing proper cyber-base hygiene, appropriately responding to cyber-attacks, and protecting confidential data.

3.4 Impacts of individual incidents and technology

Five papers relate to impacts of individual incidents and technology.

Henshaw and Van Barneveld (2016) conclude that cyber physical systems (CPS) are changing the nature of threats as they increase levels of complexity that individuals have to face; the effects of growing levels of autonomous machine decision-making in networks and added complexity in CPS bring new vulnerabilities and associated threats, with e.g. vast amounts of personal information stored in many databases.

Freeman (2018) discusses the future of drones and drone delivery, and concludes that to alleviate concerns, companies that are testing commercial drones should share with the public what information the on-board components capture and justify its need in improving drone delivery of packages. Legislation, such as who should be held accountable, and where is the line between public and private concern of the impacts of CPS may be difficult to determine (Henshaw & Van Barneveld, 2016).

Yan et al. (2018), note that ordinary users tend to be the weakest link in cybersecurity; understanding the weakest link phenomenon can help create and implement more effective cybersecurity awareness and intervention programs for ordinary users, who are the majority of society. Riek (2017) finds that, when users perceive the risk of cybercrime they become less willing to use unknown websites, or shop and bank online;

cyber policy makers can establish trust marks, standards, security certificates, and other such incentives that facilitate usage of online services.

Miftha, Conrad and Gibson (2019) call for initiatives that raise public awareness of communications being increasingly mediated via different technologies, which create possibilities of being cyber stalked. Preventative legal and technical support mechanisms recognizing possible secondary effects and negative impacts, should complement social reforms.

3.5 Cybersecurity awareness

Seven papers discuss awareness building and training.

Wilk (2019) proposes a curriculum for a course in computers, ethics, law, and public policy, which issues are very relevant to building and using intelligent systems; computer professionals and decision makers learn ethics and law fundamentals for increased professional responsibility, as future computing jobs will require technical knowledge coupled with legal and ethical awareness to cover relevant topics and challenges that tomorrow's computer professionals and decision makers will face.

Dewar (2018) notes that due to the development of digital technologies and ICT tools, cyber-attacks are prevalent, and calls for training in cyberdefense; early and clear goal definition and effective planning are key in implementing successful exercises, where scenarios, when used, should be realistic, and all exercises should serve clearly defined purposes; conducting exercises for the sake of conducting exercises becomes counterproductive.

Østby, Lovell, and Katt (2019) suggest a three-phase process that helps prepare for cyber exercises. First, the societal impact of the cyber crisis are identified; Second, roles and responsibilities of cyber crisis management are identified; Third, relevant training team roles are built; strategic approaches and excellent training skills are required to train and develop teams that are diverse in competence, measured by maturity testing before and after exercises.

According to Aaltola and Taitto (2019) building resilience, preparedness, and responding to crisis require multidisciplinary approaches, because the cyber domain crosscuts all functions of today's organizations and society, and how humans behave and how they make decisions play a crucial role in building cyber security, and training and exercises should simulate this reality as accurately as possible; considering experiential learning principles can deepen the level of learning in cyber education and training, and developing the skills and competences needed to safely navigate the cyber domain, should be seen as a constructive process, utilising and are recognising learners' previously adapted competences.

Pouraimis et al. (2019) results indicate that awareness reduces risk, as does the nature of the organisation, e.g. in military organizations people are more likely to closely follow cybersecurity protocols; significant damage can be caused depending on what resources are compromised, so potential risks that could negatively affect end-user operations should be studied and an awareness approach can have significant improvements in long term lasting risk reduction.

Alotaibi (2019) sees training of users as essential to increase awareness about cybersecurity, and that serious games as a training method can be effective in providing user training and achieving a behavioural change.

3.6 Cybersecurity and collaboration

Two papers look at creating common understanding of cyber security.

Urgessa (2020) sees that international cooperation in cybersecurity has been difficult, because the subject has been defined and conceptualized differently, and that there is incompatibility in how the respective political systems of major cyber powers have been organized; in the west, cybersecurity is mostly seen as when the machine is secure, so are the societal functions that the machine runs, while China and Russia see cybersecurity as the security of the machine, of the state, as disseminating information can threaten their political systems.

Vishik, Matsubara and Plonk (2016) note that technology and services are rapidly changing and evolving, so cyberspace related policymaking must be innovative to support growth, security, trust, confidence, and stability in society; bringing all relevant stakeholders, from government, industry, academia, to civil society, to work together in ensuring that the benefits of cyberspace are accessible to citizens; governments develop policies, strategies, and regulate the development of cyber security, while industry deploy novel technologies.

4. Discussion and conclusions

The discussion on Social and societal impacts takes a broader approach to cyber security than just national security by considering wider economical and societal impacts of digitization. The Internet and connected technology platforms enable an increase of cyber influence, which has increased the importance of awareness, while technology can aid detection and support cyber awareness. Defending national infrastructure from cyberattacks, while protecting information, networks and grids, and safeguarding citizens, property, and ecosystem services becomes a focus.

Fusion of technology into our everyday lives encourages cyber-crime, which causes an increasing need to address cyber-security vulnerabilities, and corporate accountability and human-oriented approaches help understand detrimental implications for businesses and society. Governmental oversight aids in managing the impacts that new innovations may have on society and the on lives of its members.

Detection of cyber-crime and incidents calls for data-driven innovations and analytics of big data improve event detection, situational awareness, and decision-making so that resources can be allocated efficiently, and cybercrime and other illicit use of information and communications technology (ICT) can seriously infringe the wellbeing of individuals, organizations, and society, calling for innovative managerial, technological and strategic cyber security solutions. The direct consequences of cybercrime and cyber-attacks have significant impacts and costs to economic functions, thus data collection of agent-level costs and social impacts of cyber-crime are needed to understand the impacts that cyber-attacks may have on national security.

The literature on critical services and infrastructures note that attacks on information systems can affect vital services and critical infrastructures, and protection of society and people's well-being is a governmental concern. There have been unprecedented rates of health care data breaches on organizational, business process, and technological security levels. Challenges associated with developing economically quantifiable risk assessment methods or frameworks require understanding what potential consequences are related to critical infrastructure. Identifying relevant dependencies may be based on existing security plans and service level agreements. People seem to be unaware of the risk of being attacked, while organizations need to maintain their security goals to prevent the attacks proper cyber-base hygiene and protection of confidential and sensitive data to appropriately respond to cyber-attacks are needed.

Impacts of incidents and individual technology include cyber physical systems (CPS) that are changing the nature of safety and security threats, and bring new vulnerabilities and associated. Ordinary users tend to be the weakest links in cybersecurity, and understanding this phenomenon can help create, and implement more effective cybersecurity awareness and intervention programs for ordinary users, who are the majority of society. Perceiving the potential risk of cybercrime can decrease willingness to use unknown websites, to shop, or to bank online. Cyber policy makers establish digital literary campaigns, trust marks, standards, security certificates, and other incentives to facilitate usage of online services. These initiatives raise public awareness of communications, which are increasingly mediated via different technologies. Using these technologies creates the possibility of cyber crime, often facilitated through no action of the victim. Preventative legal and technical support mechanisms recognizing possible secondary effects and negative impacts, can complement social reforms.

Cyber security awareness includes understanding computers, ethics, law, and public policy, which are very relevant to building and using intelligent systems. Computer professionals and decision makers should learn to link technical knowledge with legal and ethical awareness to cover relevant topics and challenges. Understanding the context of unique cyber-exercises, where realistic scenarios can help serve clearly defined purposes. Strategic approaches and excellent training skills are required to train and develop diverse teams, where individuals vary in competence. Proficiently predicting social media security and privacy practices assist organizations to focus on improving end-user awareness, skill and ability for better security and privacy

behavior. Building resilience, preparedness, and responding to crisis require multidisciplinary approaches, and training, where exercises can simulate reality as accurately as possible, and so better conceptualize cyber security training, education and exercises.. Awareness approaches can improve long-term lasting risk reduction. Training users is essential in increasing awareness about cyber security. Serious games can effectively provide user training to achieve behavioral change.

Regarding cyber security and collaboration, international cooperation in cybersecurity has been difficult, because there has not been common conceptualization of cybersecurity. Technology and services are rapidly changing and evolving, also cyberspace related policymaking must be innovative and support growth, security, trust, confidence, and stability in society. To achieve international harmonization, better coherence create a common context that supports multi-stakeholder interactions can enable a multi-disciplinary scientific view of cyber security that helps model needed change in cyberspace.

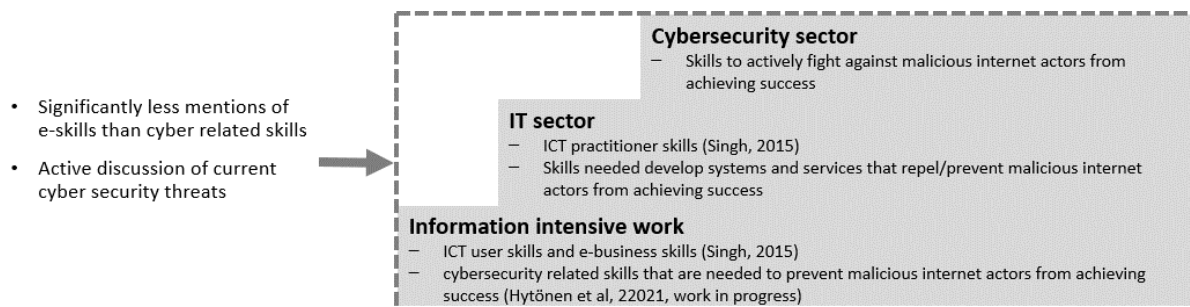


Figure 1: Cybersecurity literature focus on the workplace on levels of IT users, and IT and cyber experts

The sample literature discusses developing organizational cybersecurity focusing on the people working in information intensive jobs, where IT is used daily, and on the ITC and cybersecurity expert levels (Figure 1). ITC users may often have access rights that may put organizational information and systems in jeopardy. Distinguishing between these different user groups helps promote the skills development for successful cybersecurity.

Further study is recommended to better understand what cyber and IT-related e-skills are needed to detect, minimize and prevent possible cyberincidents. Limiting the effects of cyber incidents may directly and indirectly have wider impacts on society. Developing methods to further assess societal impacts, and e-skills and training gaps provide organizations with very practical tools to identify relevant training and recruitment needs, and understand the societal effects of cybersecurity. This could allow individuals to identify and develop their job relevant e-skills. This accumulation of practical data can contribute to science and deepen theoretical understanding.

References

- Aaltola, K., & Taitto, P. (2019). Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training.
- Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019, February). Cyber Security Goal's, Issue's, Categorization & Data Breaches. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 397-402). IEEE.
- Afonasova, M. A., Panfilova, E. E., Galichkina, M. A., & Ślusarczyk, B. (2019). Digitalization in economy and innovation: The effect on social and economic processes. *Polish Journal of Management Studies*, 19.
- Allianz Risk Barometer (2020). Available: <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyber-incident.html>
- Alotaibi, F. F. G. (2019). Evaluation and Enhancement of Public Cyber Security Awareness (Doctoral dissertation, University of Plymouth).
- Bradshaw, D. J. (2018). Technology Disruption and Blockchain: Understanding Level of Awareness and the Potential Societal Impact (Doctoral dissertation, Dublin, National College of Ireland).
- Chamie J. (2020) World population 2020: Overview. Yale Global Online, February 11, 2020. Available: <https://yaleglobal.yale.edu/content/world-population-2020-overview>.
- Cuquet, M., Vega-Gorgojo, G., Lammerant, H., & Finn, R. (2017). Societal impacts of big data: challenges and opportunities in Europe. arXiv preprint arXiv:1704.03361.
- Dewar, R. S. (2018). Cybersecurity and cyberdefense exercises. ETH Zurich.
- ECHO (2020). the European network of Cybersecurity centres and competence Hub for innovation and Operations Webpage. Available: <https://echonetnetwork.eu/>

- Freeman, E. (2018). The societal issues of drone delivery on public behaviour in the UK (Doctoral dissertation, Cardiff Metropolitan University).
- Gañán, C. H., Ciere, M., & van Eeten, M. (2017, October). Beyond the pretty penny: the Economic Impact of Cybercrime. In Proceedings of the 2017 New Security Paradigms Workshop (pp. 35-45).
- Glisson, W., & Choo, R. (2017). Introduction to Cyber-of-Things: Cyber-crimes and Cyber-Security Minitrack.
- Henshaw, M., & Van Barneveld, J. (2016). CPS for community security and safety. Ethical Aspects of Cyber-Physical Systems. Brussels: European Parliamentary Research Services STOA, 64-74.
- Ibrahim, A., Mahmud, N., Isnin, N., Dillah, D. H., & Dillah, D. N. F. (2019). Cyber Warfare Impact to National Security- Malaysia Experiences. *KnE Social Sciences*, 206-224.
- Kallberg, J., & Burk, R. A. (2014). Failed Cyberdefense: The Environmental Consequences of Hostile Acts. *Military Review*, 94(3), 22.
- Kitchenham B. (2004). Procedures for Performing Systematic Reviews. *Keele University* 33:1-26.
- Akbari Koochaksaraee, A. (2019). End-User Security & Privacy Behaviour on Social Media: Exploring Posture, Proficiency & Practice (Doctoral dissertation, Université d'Ottawa/University of Ottawa).
- Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Risk assessment of multi-order dependencies between critical information and communication infrastructures. In *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (pp. 153-172). IGI Global.
- La Torre, M., Dumay, J., & Rea, M. A. (2018). Breaching intellectual capital: critical reflections on Big Data security. *Meditari Accountancy Research*.
- McLeod, A., & Dolezel, D. (2018). Understanding Healthcare Data Breaches: Crafting Security Profiles.
- Michel, M. C. K., & King, M. C. (2019, November). Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In 2019 IEEE International Symposium on Technology and Society (ISTAS) (pp. 1-7). IEEE.
- Miftha, A., Conrad, M., & Gibson, M. (2019). Cyber stalking is a social evil: from the Indian women's perspective.
- Pouraimis, G., Thanos, K. G., Grigoriadis, A., & Thomopoulos, S. C. (2019, May). Long lasting effects of awareness training methods on reducing overall cyber security risk. In *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII* (Vol. 11018, p. 110180N). International Society for Optics and Photonics.
- Rajamäki, J., & Knuutila, J. S. (2015, November). Cyber Security and Trust. In *KMIS* (pp. 397-404).
- Rajaonah, B. (2017). A view of trust and information system security under the perspective of critical infrastructure protection.
- Riek, M. (2017). Towards a Robust Quantification of the Societal Impacts of Consumer-facing Cybercrime (Doctoral dissertation, Westfälische Wilhelms-Universität Münster).
- Schia, N. N., & Gjesvik, L. (2018). Managing a Digital Revolution-Cyber Security Capacity Building in Myanmar.
- Singh, S. (2012). Developing e-skills for competitiveness, growth and employment in the 21st century: The European Perspective. *International Journal of Development Issues*, Emerald Group Publishing, 11(1):37-59.
- Steiger, S., Harnisch, S., Zettl, K., & Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy*, 3(1), 77-95.
- Tarafdar, M., Gupta, A., & Turel, O. (2015). Special issue on 'dark side of information technology use': an introduction and a framework for research. *Information Systems Journal*, 25(3), 161-170.
- Touhiduzzaman, M., Gourisetti, S. N. G., Eppinger, C., & Somani, A. (2019, November). A Review of Cybersecurity Risk and Consequences for Critical Infrastructure. In 2019 Resilience Week (RWS) (Vol. 1, pp. 7-13). IEEE.
- Urgessa, W. G. (2020). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. *Computer Law & Security Review*, 36, 105368.
- Vishik, C., Matsubara, M., & Plonk, A. (2016). Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. NATO CCD COE Publications, Tallinn, 221-242.
- Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, 84, 375-382.
- Yanakiev, Y. (2020). A governance model of a collaborative networked organization for cybersecurity research. *Information & Security*, 46(1), 79-98.
- Wilk, A. (2019). Teaching AI, Ethics, Law and Policy. arXiv preprint arXiv:1904.12470.
- Østby, G., Lovell, K. N., & Katt, B. (2019, December). EXCON teams in cyber security training. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 14-19). IEEE.