Measuring Societal Impacts of Cybersecurity

Jarmo Heinonen and Harri Ruoslahti
[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland

Jarmo.heinonen@laurea.fi
Harri.ruoslahti@laurea.fi

Abstract: Cybersecurity is more important than ever. All facets of society, including critical sectors such as financial, healthcare, energy, and transportation, are very reliant on cyberspace. Information and communications technology have become more and more relevant in organizations and are crucial elements in organizational learning and networked development and resilience. This study focuses on the analysis and findings of a cybersecurity questionnaire on the quantitative side of the survey contemplate mainly cybersecurity competences of the personnel in the participants' companies. The data was analysed with principal component, correspondence analysis, and the Euclidean distance two-dimensional figures. The extraction method was Principal component analysis to extract 11 factors, with more than 25 iterations. Correspondence analysis shows that the private and public non-authority sectors prefer workers with communication and collaboration skills and an ability for situational awareness. Private subsidiaries prefer leadership skills. The results show that the Societal Impact Assessment Toolkit questionnaire can be used in organizations or projects to assess the societal impact of their cybersecurity products and services. The questionnaire will be developed to-ward a standardized method, which will require collecting answers from larger numbers of respondents for further evaluation and testing it with ap-propriate qualitative methods. This will add to the body of knowledge on the societal impacts of cybersecurity. The tool is a very practical contribution for companies, while the continued use and the ensuing analysed data that be-comes collected from large numbers of respondents becomes a contribution to theory.

Keywords: Societal Impact, Assessment, Cybersecurity

1. Introduction

Society is more connected than ever, as all its facets, including critical sectors such as financial, healthcare, energy, and transportation, rely very heavily on cyber-space (Tagarev & Davis, 2020). Modern information and communications technology (ICT) solutions and infrastructures are vulnerable to cyberattacks that leverages malware, phishing, machine learning or artificial intelligence, and may target individual, organizational, and state levels (Maglaras et al., 2018; Stellios et al., 2028), calling for investments in cyber-security, which are at an all-time high Morgan, 2019).

The "Cybersecurity Competence Network", a European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO), was one of four pilot projects of 30 partners from 14 European countries from different sectors including healthcare, transport, manufacturing, ICT, education, research, telecom, energy, space, defence, civil protection, public, and private organizations. (ECHO network, 2020). The project Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) develops a platform where artificial intelligence-based (AI) approaches combine business continuity management (BCM) and cyber threat intelligence (CTI) to deal with increasing digitalisation with resilience assessment and awareness to minimize the number of cyberattacks against the critical sectors of society (DYNAMO project, 2023).

One key cybersecurity challenge is preparing for future risks and finding ways to respond to new emerging types of attacks, while concurrently. Understanding what potential impacts cybersecurity, or the lack of, may have on society and its members will help make relevant decisions on how to plan and prepare against cyber threats and what cybersecurity investments should be made. The research question of this study is: What are the Societal Impacts of Cybersecurity?

2. Literature Review

This section discusses how information and communications technology have become more and more relevant in organizations and have become crucial elements in organizational learning and networked development. This section also discusses resilience and preparedness against the many possible cyber threats to better under-stand what impacts cybersecurity may have on society.

2.1 Information and Communications Technology in Organisations

Ruoslahti and Trent (Ruoslahti & Trent, 2020) find four main themes of consideration of information and communications technology (ICT) implementation, which are ICT alignment, Organizational Culture, Innovation Culture, and ICT-readiness. ICT can be in a critical element in promoting innovation (Lu et al., 2019) and in supporting decision-making and transforming business processes (Cupiał et al., 2018), and business survival may even depend how well new IT are implemented, and the opportunities that they bring being taken advantage of (Hernandez, Jimenez & Martin, 2010).

ICT can promote Organizational Learning as a catalyst for Knowledge Management practices (Huang, Gardner & Moayer, 2016), and as they are applied to existing processes, they serve to im-prove internal and external flows of information (Im, Porumbescu & Lee, 2013). Business strategies Information Systems strategies should align so that the development and usage of IT-infrastructures are clear for all members of the organization (Choe, 2016). Building modern competitiveness is increasingly reliant on ICT-implementation (Mihalic & Buhalis, 2013), as ICT offers opportunities for strategic and distance learning (Lopez-Nicolas & Soto-Acosta, 2010).

Learning is necessary in modern organizations (Lemmetty & Collin, 2019), and mobile technologies have brought new opportunities to the education sector (Turi, 2019). Organizational Culture plays an integral role in successful ICT integration (Ruoslahti & Trent, 2020), while leadership can and should promote positive policies and sense of readiness, to minimize change resistance (Cha, Hwang & Gregor, 2015), and ICT makes it easier to store and share organizational knowledge (Siddiqui et al., 2019).

As ICT plays a prominent role on organizational knowledge management, their processes, services, and product innovation become strongly influenced by the used ICT-tools, and these shape organizational cultures (Siddiqui et al., 2019). Innovation culture can bene-fit from consolidating the strengths of blended e-learning and traditional face-to-face interactions to increase quality, effectiveness, efficiency, and abilities (Conková, 2013).

Because ICT is instrumental in supporting knowledge sharing, by lowering communication barriers and promoting collective behaviours, building adequate ICT-support is critical for organizational knowledge management systems (Rahman, Islam & Abdullah, 2017). protecting ICT-systems against threats is highly significant for the overall availability of the critical systems that support organizational processes, and to ensure the availability of digital information calls for risk assessment (RA) based measures (Pöyhönen et al., 2020).

2.2 Networked Development

When people work towards common objectives that affects their communities, they become more responsible, which promotes social learning (Webler, Kastenholz & Renn, 1995), and as innovation is based on new knowledge, it can drive growth and success (Dandonoli, 2013; Burdon, Mooney & Al-Kilidar, 2015). Co-creation is a collaborative activity with determined objectives, arenas, collaborators, tools, processes, and contracts (Bhalla, 2014), which takes place on different layers, involving agents to co-create policies and futures (Accordino, 2013), to generate new knowledge and skills resulting to innovations (Henriksson, Ruoslahti & Hyttinen, 2018; Ruoslahti, 2018).

Co-creation of knowledge can combine physical spaces and digital environments or occur in one or the other (Bhalla, 2014), as actors meet in these physical or digital spaces to address and discuss issues that are relevant to them, communication can be seen to take place in these Issue Arenas (Vos, Schoemaker & Luoma-aho, 2014). These arenas can be competitive spaces, where actors have both common agendas and interests of their own and where they use problem solving and influencing strategies (Saarinen, 2012; Vos, 2018).

Linkov, et al. (2014) find that critical infrastructures may typically lack resilience, which can cause them to lose essential functionalities if hit by adverse events. Successful crisis-management enables organizations prepare to sustain and resume operations, and to minimize losses, and adapt to manage future incidents (Linkov et al., 2013). Effective response to disturbances and collaboration during those disturbances depend heavily on shared situational awareness (Pöyhönen, 2020).

Ruoslahti, Rajamäki & Koski (2018) note that considering resilience event management cycles, such as plan or prepare, absorb, recover, adapt, and learn, and self-modify, may help plan measures to ensure the continuity of Cyber Physical Systems (CPS), which are composed of cyber, technical, social and ecological systems. Organizational resilience includes conditions and to understand and reduce risks and mitigate crises (Vos, 2017), and prior knowledge of critical infrastructure sectors, experiences of CPS, and avail-able best practices can help design and maintain resilience (Pöyhönen, 2020; Ruoslahti, 2018).

2.3 Societal Impacts

De Jong et al. (2014) highlighted that societal impact can be understood through interactions and as product, knowledge use, and direct benefit to society. Societal im-pacts as a product shows potential societal value when used by societal audiences as a product, which can also be a service, information, tool, instrument, method, or model (Shapiro, 2007). Societal impacts as knowledge use can include interactions between societal stakeholders that result in the adoption or use of knowledge, which may, or may not be, facilitated by a product (Castro Martínez, Molas Gallart & Fernández de Lucio, 2008). Societal benefits to society can be use of innovation research results, policies, practices, jobs, education, community formation, network building, trust that have impacts on culture, media, and community (Walter et al., 2007).

The Internet and connected technologies have increased cyber influence, cyber-crime, behaviours, and actions that may impact personal privacy corporate and nation-al security (Michel & King, 2019). The ramifications of cybercrime go beyond may go the consequences inflicted by cyber-attacks themselves, and economies could be impacted with significant costs (Gañán, Ciere & van Eeten, 2017). A cyber-attack may even lead to environmental damage, which in turn could have detrimental effects on the stability of society (Kallberg & Burk, 2014).

Economic and societal developments increasingly rely on digitalization and ICT, and this adds to the need for Cyber Security to protect these benefits (Schia & Gjesvik, 2018). Personal data, for example, are increasingly harvested and sold, so maintaining an explicit awareness of what is real, and fake is a key safeguard from cyber influence and harm; technology can help detect and support awareness of personal privacy or national security harm related influence (Michel & King, 2019). Defending all levels of infrastructures from cyber-attacks means that information, network availability, and information grids are protected, to preserve ecosystems and ecosystem services, while safeguarding the people's property and lives (Kallberg & Burk, 2014).

Though societies may be aware of most emerging technologies and with the potential of disruptions, they may still fail to understand what impacts these innovations may have on society or the lives of its citizens (Bradshaw, 2018). Effective, economic and impact evaluations require systematically collecting accurate reliable data on agent-level costs of cybercrime, where analysis and information become based on pre-set factors and indicators that better understanding of the respective impacts to support decision-making and cyber security investments (Gañán et al., 2017). Policy makers should prepare for an upcoming technology-driven disruption of society, as this 'dark side' of IT has the potential to violate the wellbeing of individuals, organizations, and societies (Tarafdar, Gupta & Turel, 2015).

3. Method

This study serves as a pilot study of the ECHO Societal Impact Assessment Toolkit questionnaire. The aim of the study is to understand the societal impacts of cybersecurity as a selected case study of the D9.15 ECHO deliverable. A secondary aim is to verify the questions of the Toolkit questionnaire. This study focuses on the analysis and findings of organizational cybersecurity structures and substructures, and the competencies needed on different task levels to build comprehensive cyber-security.

Developing the 73 survey questions for the Societal Impact Assessment Toolkit were based on the main research question and a prior empirical study on expert views on Cyber Range (CR) capabilities, interactions and features in acquisition of cyber skills. The context of the Toolkit questions is cybersecurity skills, where the cybersecurity related backgrounds of respondents form a sample of relevant companies and organizations.

The Toolkit has open-ended and multiple-choice questions that use a five step Likert scale of cybersecurity alternatives. ECHO partner experts working in the field of cybersecurity were asked to check and comment the first version of the Toolkit questionnaire questions. The sample size did not quite reach the goal of a hundred respondents. The final sample (n = 81) was less than expected but deemed sufficient to conduct this pilot study as more answers proved difficult to obtain. All questionnaires that were not completed in full were left out of the analysis.

Background data are first collected in the beginning of the questionnaire to collect personal and organizational information. The quantitative questions of the sur-vey focus on cybersecurity choices and competences of the personnel in the participating companies.

The data was analysed with principal component analysis to find out groups in which one of the loadings are connected (Principal component analysis and Kaiser normalization, cutting point 0,25). The highest loadings from the same component that were focused as the most meaningful were analysed by correspondence analysis

with two variables. The Likert scale questions were analysed with correspondence analysis and the Euclidean distance two dimensional figures. The Euclidean distance can be calculated with Pythagorean theorem (d(p,q)2 = (q1-p1)2+ (q2-p2)2) in two-dimensional space. Correspondence analysis is an exploratory multivariate technique that converts a data matrix into a particular type of graphical display in which the rows and columns are depicted as points (Yelland, 2010; Greenacre & Hastie, 1987).

Besides two-dimensional graphics limitations more figures are needed to reveal additional information. For example, factor analysis or other suitable multidimensional methods are needed to reveal the best suitable variables for correspondence analysis and its graphics. The reliability of the material was analysed with Cronbach's Alpha (0,899). The open-ended survey responses were analysed with qualitative content analysis (Denzin & Lincoln, 1994).

The extraction method, Principal component analysis, provided and extraction of 22 factors after 25 iterations with the first cutting point that was set at 0,25 (Metsämuuronen 2005) in the SPSS program. The cumulative variance was mostly on the first component, so to focus on the more meaningful aspects a final cutting point was set at 0,45, which provided eleven (11) factors.

4. Results: Attributes of Collaboration Network Resilience

This section discusses the results of the qualitative and quantitative analysis of the Societal Impact Toolkit questionnaire, which has 73 questions altogether. The first five open-ended questionnaire questions deal with company background and the participant information. The remaining 68 questions are multiple choice questions on a five-step Likert scale deal with cybersecurity related choices and skills.

Two of the questions (profession and the organization) proved to be too complicated for relevant analysis. There were too many professional titles and organisational departments to categorize them appropriately. This indicates that there is a need for predetermined groups or options for respondents to choose from to these questions. This will make the questionnaire easier to answer by providing more specific title backgrounds.

The questionnaire contains 68 multiple-choice questions that deal with cybersecurity related choices and skills. Principal component analysis was used to extract eleven principal components from multiple-choice questions. Table 1 lists these principal components and shows the number of questions that they are connected to.

Table 1: Principal components.

Order of component	Name of component	Connected to n questions (over 0.45)	Connected to n questions negatively
1st	Vulnerability evaluations	16	0
2nd	European solution	3	0
3rd	Cyber-attacks	1	1
4th	Insurance	2	2
5th	Outsourced	2	2
6th	External consultants	1	0
7th	Business first	0	1
8th	Hard work	1	0
9th	Key features	1	0
10th	Who should be trained	1	0
11th	Key skills	1	0

The first component named "vulnerability evaluations" was connected to the 16 questions (table 1) : "we conduct regular vulnerability evaluations in-house " (0,664), "we have a dedicated in-house capabilities for handling cyber-attacks " (0,783), "we have dedicated budget to address cybersecurity" (0,730), "we conduct vulnerability evaluations to identify potential points" (0,784), "we conduct regular vulnerability evaluations by external providers" (0,612), "we use cybersecurity practices in a daily basis to maintain a safer environment" (0,609), "we have a dedicated budget for cybersecurity expenditure" (0,603), "we regularly have cyber exercises to identify key milestones for improvements" (0,623), "we regularly have cyber exercises to define the level of

resilience" (0,692), "we use needs based self-evaluations when purchase cyber security" (0,689), "we make cybersecurity related purchases" (0,677), "we have mandatory compliance requirements" (0,636), "business planning processes look at previous cybersecurity designs"(0,663), "we engage proactively in using cybersecurity cases" (0,679), we measure cost effectiveness of cybersecurity based n cost analyses" (0,600), and "we have a fixed budget for cyber security" (0,687).

The second component named "European solution" (table 1) was connected to three questions: "do you favour European cybersecurity solutions over non-European" (0,526), "would you purchase cybersecurity services from Europe" (0,501), and "would you use a European cybersecurity marketplace" (0,561).

The third component named "cyber-attacks" (table 1) was connected to one question "we feel threatened by cyber-attacks" (0,448), and negatively to one question: "we use cybersecurity practices in a daily basis to maintain a safer environment" (-0,483).

The fourth component named "insurance" (table 1) was connected to one question: "we will continue without cyber insurance" (0,462), and negatively connected to two questions: "we use insurance to cover certain types of cybersecurity incidents" (-0,635), and "we have insurance coverage for cybersecurity supply chain risks" (-0,558).

The fifth component named "out-sourced" (table 1) was connected to one question: "we have out-sourced partners for handling cyber-attacks" (0,490), and negatively connected to two questions: "we hire and train in-house people who have basic understanding of domain" (-0,509), and "we hire people with proven competence even without degree" (-0,464).

There were six components that related to one question each. the sixth component was named "external consultants" (table 1) connected with the question: "we purchase cyber services from security firms" (0,511). the seventh component "business first" (table 1) was connected to the question: "do you have dedicated career path for employees" (-0,475). the eighth component "hard work" (table 1) was connected to the question: "we appreciate work experience" (0,478). the ninth component was named "key features" and connected to: "what are the key features expected cyber-security service" (0,503). the tenth component "who should be trained" connected with the question: "who should be trained in cyber security in your organizations" (0,494). the eleventh was named "key skills" and connected with the question: "what are the key cybersecurity skills you seek from your employees" (0,457).

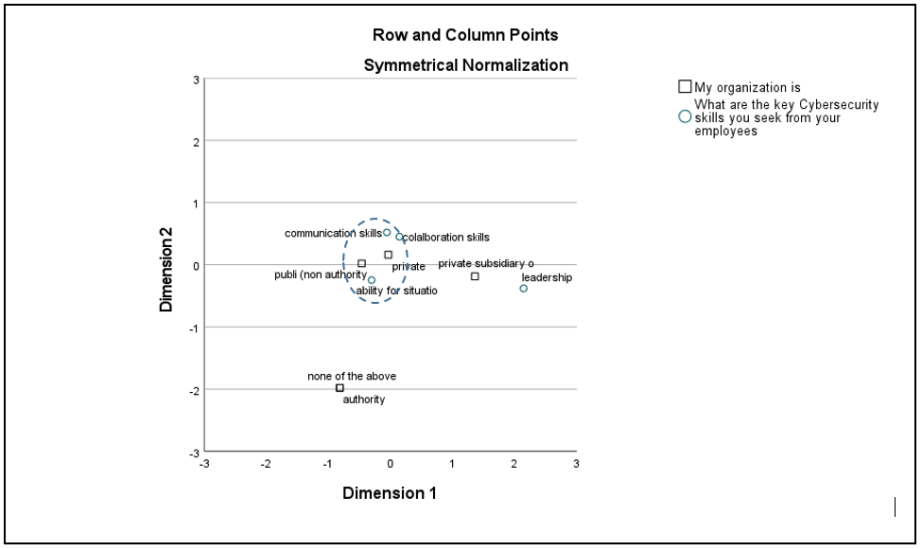

Figure 1: Correspondence analysis between key skills and organization

Figure 1 visualizes that the Correspondence analysis of the data shows that the private sector and the public-non-authority sector prefer workers who have good communication skills, collaborative skills, and an ability for situational awareness. Private subsidiary organizations mainly look for leadership skills. Public-authority organizations however differ in the way that they do not look for these above-mentioned features.

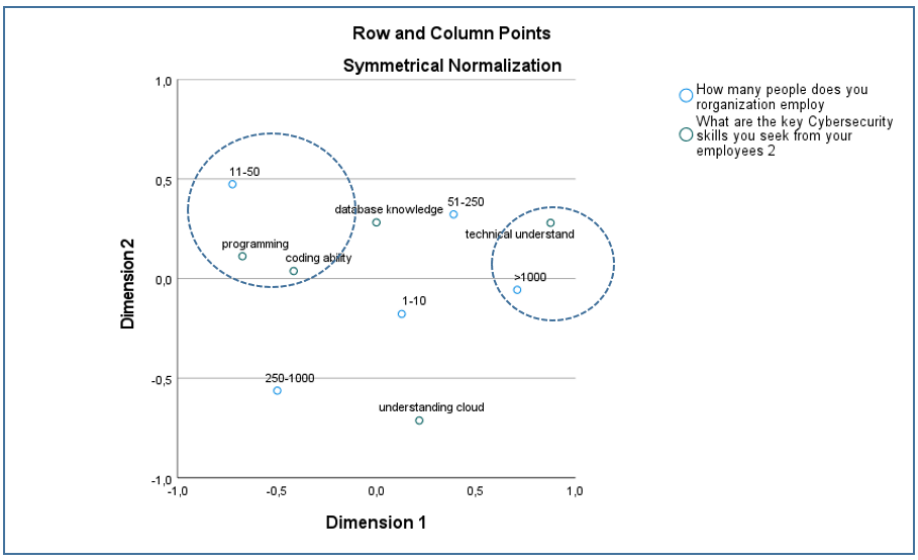

Figure 2: Key Cybersecurity skills needed in companies.

Large companies that have more than 1000 employees look for technical under-standing, while smaller companies that have between 11 and 50 employees seem to prefer programming skills and coding ability from their employees (Figure 2).

5. Conclusions

The Societal Impact Assessment Toolkit questionnaire can be used operatively. The principal component analysis shown that there are many components which affect societal impact, and the first component "Vulnerability evaluations" was connected to the 16 questions which gather the biggest quantity of variables. There are different kind of requisites how big is the company and what kind of workers they need.

The components that have relate to largest number of positive questions are "Vulnerability evaluations" (16), "European solution" (7), "Hard work" (7) and "Effectiveness" (6). Ten of the 22 identified components are related to one or two questions (cutting point 0,25). To address this, the further development of the questionnaire should be based on collecting significantly larger numbers of respondents.

The results of this study clearly indicate the need to develop the background questions on profession and the organization by providing predetermined options from which respondents can choose. This will make both answering these questions and future analysis of them easier.

The aim is to collect more respondents and further develop the Toolkit towards a standardized method with which the societal impacts of cybersecurity. To this end, the ECHO Societal Impact Assessment Toolkit questionnaire was partially based on a previous cyber-range (CR) study, and its questions were evaluated by cyber security experts and validated with relevant quantitative methods.

The Societal Impact Assessment Toolkit questionnaire can be used within organisations or projects that wish to assess the societal impact of their products and services. Developing this structured questionnaire toward a standardized method will require collecting answers from a larger sample of respondents and to further evaluate and test it with appropriate qualitative methods. When used in more quantity, this path towards a standardized method to assess the societal impacts of cybersecurity can provide a contribution to science and theory. The contribution to practice will be the availability for usage of this Societal Impact Assessment Toolkit questionnaire in future research and innovation projects. Interestingly, malware and firewalls were not mentioned. New current questions can be listed at the end of the questionnaire, if the first part remains the same and comparability with the previous one is maintained.

Though this Toolkit questionnaire purely addresses the societal impacts of cyber-security, this same approach could be adopted to similarly develop structured and standardized methods to assess other issues. These could be for example, sustainability or ethics. This would further answer a recognized need to develop easier to use analysis methods to replace some of the time and labour-intensive qualitative approaches currently used.

This questionnaire will be used to analyse societal impacts in the DYNAMO project. This pilot study under the ECHO project has been a valuable starting point. The results are expected to improve with a larger sample of respondents. In the field of security, the respondents tend to be reluctant to answer questionnaires, but rather wish to keep themselves in the dark. In time this questionnaire many be used in other future projects to provide even more responses that will further deepen the results.

Acknowledgement

This study has received funding by the European Union projects ECHO, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943, and DYNAMO, under grant agreement no. 101069601. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Accordino, F. (2013), The Futurium – a Foresight Platform for Evidence-Based and Participatory Policymaking, Philosophy & Technology, vol. 26, no. 3, pp. 321-332.

Bhalla, G. (2014). How to plan and manage a project to co-create value with stakeholders, Strategy & Leadership, Vol. 42 No. 2 2014, pp. 19-25.

Bradshaw, D. J. (2018). Technology Disruption and Blockchain: Understanding Level of Awareness and the Potential Societal Impact, Doctoral dissertation, Dublin, National College of Ireland.

Burdon, S., Mooney, G. R. and Al-Kilidar, H. (2015). Navigating service sector innovation using co-creation partnerships. Journal of Service Theory and Practice, vol. 25, no. 3, pp. 285-303.

Castro M., E., Molas G., J., and de Lucio, F., I. (2008). Knowledge transfer in the Human and Social Sciences: the importance of informal relationships and its organizational consequences.

Cha, K.J., Hwang, T. and Gregor, S. (2015). An integrative model of IT-enabled organizational transformation: A multiple case study. Management Decision, 53(8), pp. 1755-1770.

Choe, J. M. (2016). The Construction of an IT Infrastructure for Knowledge Management. Asian Academy of Management Journal, 21(1).

Conková, M. (2013). Analysis of Perceptions of Conventional and E-Learning Education in Corporate Training. Journal of Competitiveness, 5(4), n/a.

Cupiał, M., Szeląg-Sikora, A., Sikora, J., Rorat, J. and Niemiec, M. (2018). Information technology tools in corporate knowledge management. Ekonomia i Prawo, 17(1), pp. 5-15.

Dandonoli, P. (2013). Open innovation as a new paradigm for global collaborations in health. Globalization and Health, vol. 9, no. 1, pp. 1-5.

De Jong, S., Barker, K, Cox, D, Sveinsdottir, T. and Van den Besselaar, P. (2014). Understanding societal impact through productive interactions: ICT research as a case Research Evaluation 23(2), pp. 89-102.

Denzin, N. K. and Lincoln, Y. S. (1994). Handbook of Qualitative Research, Sage Publications, Thousand Oaks, USA

DYNAMO project, 2023. Dynamic Resilience Assessment Method [WWW Document]. URL https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf (accessed 1.24.24)

ECHO network (2020). ECHO network webpage (https://echonetwork.eu/, accessed November 4).

European Commission (2017). Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN/2017/0450 final https://eur-lex.europa.eu/legal-con tent/EN/ALL/?uri=CELEX:52017JC0450, accessed February 8 2021).

European Commission (2020). Europe investing in digital The Digital Europe Programme (https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-pro gramme, accessed December 15).

Gañán, C. H., Ciere, M. and van Eeten, M. (2017). Beyond the pretty penny: the Economic Impact of Cybercrime Proceedings of the 2017 New Security Paradigms Workshop October 2017, pp. 35-45.

Greenacre M. and Hastie T. (1987). The Geometric Interpretation of Correspondence Analysis. Journal of the American Statistical Association, Vol. 82, No. 398 (Jun. 1987), pp. 437-447.

Henriksson, K., Ruoslahti, H., and Hyttinen, K. (2018). Opportunities for strategic public relations - evaluation of international research and innovation project dissemination. In Bow man, S. Crookes, A., Romenti, S. & Ihlen, Ø (eds.). Public Relations and the Power of Creativity (Advances in Public Relations and Communication Management, Volume 3).

Hernandez, B., Jimenez, J. and Martin, M.J. (2010). Business management software in high tech firms: the case of the IT services sector. The Journal of Business & Industrial Marketing, 25(2), pp. 132-146.

Huang, F., Gardner, S. and Moayer, S. (2016). Towards a framework for strategic knowledge management practice: Integrating soft and hard systems for competitive advantage Very In formal Newsletter on Library Automation. VINE Journal of Information and Knowledge Management Systems, 46(4), pp. 492-507.

Im, T., Porumbescu, G., and Lee, H. (2013). ICT as a buffer to change: A case study of the Seoul Metropolitan Government's Dasan Call Center. Public Performance & Management Review, 36(3), pp. 436-455.

Kallberg, J. and Burk, R. A. (2014). Failed Cyberdefense: The Environmental Consequences of Hostile Acts Military Review 94(3), 22.

Lemmetty, S., and Collin, K. (2019). Self-Directed Learning as a Practice of Workplace Learning: Interpretative Repertoires of Self-Directed Learning in ICT Work. Vocations and Learning, pp. 1-24.

Linkov, I. et al. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp. 471-476.

Linkov, I. et al. (2014). Changing the resilience paradigm. Nature Climate Change, Volume 4, pp. 407-409.

Lopez-Nicolas, C. and Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs: SSIS. International Journal of Information Management, 30(6), 521.

Lu, H., Pishdad-Bozorgi, P., Wang, G., Xue, Y. and Tan, D. (2019). ICT Implementation of Small- and Medium-Sized Construction Enterprises: Organizational Characteristics, Driving Forces, and Value Perceptions. Sustainability, 11(12), 3441.

Maglaras, L., Ferrag. M, Derhab, A., Mukherjee, M., Janicke, H. and Rallis, S. (2018) Threats, countermeasures and attribution of cyber-attacks on critical infrastructures EAI Endorsed Transactions on Security and Safety 5 (16).

Michel, M. C. K. and King, M. C. (2019). Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. 2019 IEEE International Symposium on Technology and Society (ISTAS), November 2019, pp. 1-7.

Mihalic, T. and Buhalis, D. (2013). ICT as a New Competitive Advantage Factor - Case of Small Transitional Hotel Sector. Economic and Business Review for Central and South-Eastern Europe, 15(1), 33-56

Morgan, S. (2019). Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021, Cybercrime Magazine June 10 2019.

Pöyhönen, J., Rajamäki, J., Lehto, M. and Ruoslahti, H. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. Annals of Disaster Risk Sciences, Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure. Available: https://ojs.vvg.hr/in dex.php/adrs.

Rahman, S., Islam, M. Z., and Abdullah, A. D. A. (2017). Understanding factors affecting knowledge sharing. Journal of Science and Technology Policy Management.

Ruoslahti, H. 2018. Co-creation of Knowledge for Innovation Requires Multi-Stakeholder Public Relations. In Bowman, S., Crookes, A., Romenti, S. and Ihlen, Ø. (Eds) Public Relations Public Relations. In Bowman, S., Crookes, A., Romenti, S. and Ihlen, Ø. (Eds) Public Relations and the Power of Creativity, Advances in Public Relations and Communication Management, Volume 3, Emerald Publishing Limited, 115-133.

Ruoslahti, H., Rajamäki, J. and Koski, E. (2018). Educational Competences with regard to Resilience of Critical Infrastructure. Journal of Information Warfare, 17(3), pp. 1-16.

Ruoslahti, H. and Trent, A. (2020). Organizational Learning in the Academic Literature – Systematic Literature Review. Information & Security: An International Journal 46:1, pp. 65-78.

Saarinen, L. (2012). Enhancing ICT Supported Distributed Learning through Action Design Research. Aalto University publication series, Doctoral Thesis 92 7 2012, Helsinki.

Schia, N. N. and Gjesvik, L. (2018). Managing a Digital Revolution-Cyber Security Capacity Building in Myanmar NUPI Working Paper 884, Norwegian Institute of International Affairs.

Shapiro, H., Haahr, J. H., Bayer, I. and Boekholt, P. (2007). Background paper on innovation and education Danish Technological Institute and Technopolis for the European Commission, DG Education & Culture in the context of a planned Green Paper on innovation.

Siddiqui, S. H., Rasheed, R., Nawaz, S., and Abbas, M. (2019). Knowledge sharing and innovation capabilities: The moderating role of organizational learning. Pakistan Journal of Commerce and Social Sciences (PJCSS), 13(2), pp. 455-486.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018). A survey of IOT enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Communications Surveys & Tutorials 20 (4), pp. 3453-3495.

Tagarev, T. and Davis, B. Á. (2020). Towards the Design of a Cybersecurity Competence Network: Findings from the Analysis of Existing Network Organisations International Conference on Multimedia Communications, Services and Security (Springer, Cham), pp. 37-50.

Tarafdar, M., Gupta, A. and Turel, O. (2015). Special issue on dark side of information technology use: an introduction and a framework for research Information Systems Journal 25(3), pp. 161-170.

Turi, J. A., Javed, Y., Bashir, S., Khaskhelly, F. Z., Shaikh, S., and Toheed, H. (2019). Impact of Organizational Learning Factors on Organizational Learning Effectiveness through Mobile Technology. Quality-Access to Success, 20(171).

Vos, M. (2017). Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience, Jyväskylä: Jyväskylä University School of Business and Economics.

Vos, M. (2018). Issue Arenas. In Heath, R. and Johansen, W. (Eds.), The International Encyclopedia of Strategic Communication (IESC). Whiley Blackwell, Malden MA.

Vos, M., Schoemaker, H. and Luoma-aho, V. L. (2014). Setting the agenda for research on issue arenas. Corporate Communications: An International Journal, Vol. 19 No. 2, 2014. Emerald Group Publishing Limited, pp. 200-215.

Walter, A. I., Helgenberger, S., Wiek, A. and Scholz, R. W. (2007). Measuring societal effects of transdisciplinary research projects: design and application of an evaluation method Evaluation and program planning 30(4), pp. 325-338.

Webler, T. Kastenholz, H. and Renn, O. (1995) Public Participation in Impact Assessment: A Social Learning Perspective. in Environmental Impact Assessment Review 15(5), 443-463 · September 1995. https://doi.org/10.1016/0195-9255(95)00043-E.