Societal Impacts of Cyber Security Assets of Project ECHO

HARRI RUOSLAHTI[1], BRÍD DAVIS[2]
[1]Laurea University of Applied Sciences, FINLAND
[2]The National University of Ireland, Maynooth, IRELAND

Abstract:- Solutions on both consumer and state levels have become increasingly vulnerable to sophisticated cyberattacks by e.g. malware, phishing, machine learning and artificial intelligence. As the adoption and integration of information technologies are increasing and solutions are developing, the need to invest in cyber-security is at an all-time high. Investment in cybersecurity is a chief priority within the European Union, and project ECHO is a one initiative that put emphasis on devising, elaborating, implementing and enhancing a series of technological solutions (assets) to counteract cyber-attacks. The research problem of this study is what societal impacts do the ECHO assets have as product, as knowledge use, and as benefits to society. The literature review includes theory and practice from academic papers, EU innovation project and professional reports, and some ECHO project workflows. Relevant academic theoretical approaches that provide a basis for this task are: e-skills and training, Organisational Learning (OL), Societal Impact (SI), Societal Impact Assessment (SIA). This is a qualitative pilot study that evaluates the usefulness of employing a Product/ Knowledge/ Benefit Societal Impact framework to assessment of societal impacts. Data collection involved qualitative participatory observation of a co-creative expert hackathon workshop. This pilot study shows that the methodology path, where societal impact of ICT and AI solutions (e.g. the ECHO assets) are examined as these three elements (product, knowledge use, societal benefit). This pilot study serves as a step to validate this path and design and select practical, rigorous and relevant quantitative methodology to further the understanding of both societal impact assessment of cyber, e-, and AI-based solutions and services. To incorporate societal impacts with cyber and e-skills this study recommends developing and refining actual key performance indicators (KPI) to provide a basis for rigorous and relevant qualitative and quantitative questionnaire based inquiry of cyber, e-, and AI-based solutions and services.

Key words: - Artificial Intelligence, Cybersecurity, E-skills, Societal Impact Assessment

Received: June 12, 2021. Revised: November 15, 2021. Accepted: December 8, 2021. Published: December 30, 2021.

1 Introduction

Living in the 'smart technology era', as a society have never been more connected. Indeed, there has been an exponential shift globally wherein all facets of society are relying on cyberspace – including, but not limited to - the financial, healthcare, energy and transportation sectors [1]. Yet, such solutions and infrastructures (whether at a consumer or state level) are vulnerable to sophisticated cyberattacks leveraged by malware, phishing, machine learning and artificial intelligence, etc. [2; 3; 4]. Consequently, while the adoption and integration of information technologies are commendable, investment in cyber-security is at an all-time high [5].

Currently, the global cyber-security market is valued at more than $150 billion, with the market size projected to surpass $400 billion by 2026 [6]. While the largest market share is positioned in the United States, which equated to 36.1% in 2019, [7], the Digital Europe Programme, scheduled roll-out between 2021-2027, involves a significant investment of €1.9 billion into cybersecurity capacity and the wide deployment of cybersecurity infrastructures and tools across European Union (EU) states [8].

Undoubtedly, investment in cybersecurity is a chief priority for the European Union. In 2018 the European Parliament and the Council issued a proposal for establishing a European cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres [8]. A call for proposals via the Horizon 2020 programme was issued in parallel, aiming to overcome the fragmentation of EU research capacities and ensure that "the EU retains and develops the essential capacities to secure its digital economy, society and democracy" [9].

One of the objectives of the call was to establish and operate a pilot for a "Cybersecurity Competence Network", a European network of Cybersecurity centres and competence Hub for innovation and Operations [10]. The ECHO consortium - one of four pilot projects - consists of 30 partners from 14 European countries which align with different fields

and sectors including healthcare, transport, manufacturing, ICT, education, research, telecom, energy, space, defence & civil protection (public and private, for-profit and non-for-profit organisations). ECHO puts a particular emphasis on devising, elaborating, implementing and enhancing a series of technological solutions (assets) to counteract cyber-attacks based on the ECHO project consortium.

A key cybersecurity challenge is the means of responding to new types of attacks, while concurrently preparing for future risks. One such potential solution centres on devising a series of advanced technological solutions ('assets'), which the ECHO project are developing to counteract destructive cyber-incidents as a means of early-intervention. Such solutions and technologies should not only have technical impacts, but also societal impacts.

The ECHO project will in part develop frameworks to assess the diverse aspects related the societal impact assessment for ECHO assets and governance; and a-skills and training. ECHO aims to devise an easy-to-use assessment measure, which could be used to sustain and improve the assessment skills and will be based on relevant requirements, policies, analysis, EU guidelines, frameworks and certification.

Accordingly, the ECHO project is developing six assets (Figure 1) while striving to devise a network of cyber-research and competence centres. Thus, while collaborating with other funded cyber research networks, there is also a mandate to increase participation with a new partner engagement model. Moreover, in an effort to address European cyber security gaps, the project is in the process of developing an adaptive model for information sharing and collaboration among the wider network of cybersecurity centres. This is accomplished within a multiple-sector context, supported by a framework for improved cyber-skills development and technology roadmap delivery, and an early warning system [10].

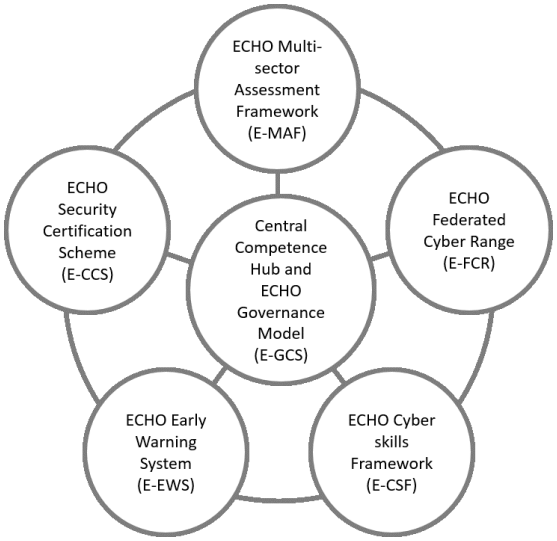

Fig. 1: ECHO Assets [10].

The ECHO project will in part develop frameworks to assess the diverse aspects related the societal impact assessment for ECHO assets and governance; and a-skills and training. ECHO aims to devise an easy-to-use assessment measure which could be used to sustain and improve the assessment skills and will be based on relevant requirements, policies, analysis, EU guidelines, frameworks and certification. The research questions of this study are:

RQ1: Identify societal impacts of the ECHO assets as product?

RQ2: Identify societal impacts of the ECHO assets as knowledge use?

RQ3: Identify societal impacts of the ECHO assets have as benefits?

2 Literature

The relevant literature for the task consists of both theory and practice derived from academic papers, EU innovation project and professional reports, and the workflows of the entire ECHO project. Relevant academic theoretical approaches that provide a basis for this task are: Organisational Learning (OL), Societal Impact (SI), Societal Impact Assessment (SIA), and E-skills and Training.

2.1 Organizational Learning

Ruoslahti and Trent [11] identified the following four themes within Information and Communications Technology (ICT) literature in relation to Organisational Learning (OL): 1) ICT alignment, 2) Organizational Culture, 3) Innovation Culture, and 4) ICT-readiness. Cupiał and colleagues [12] determined that ICT enables

companies to develop skills that enable them to absorb knowledge from external sources, even with seemingly limited resources. Additionally, ICT facilitates storing and sharing of organizational knowledge - helping employees garner new expertise [13]; ICT also acts as a catalyst for organizational learning, in which new knowledge is generated and processed thus promoting productivity and competitiveness [14].

ICT-implementation is fundamental to establishing competitiveness [15]. ICT enables rapid search, access and retrieval of information [13], enhancing strategic learning, even over distances [16]. Consequently, business success potentially depends on taking advantage of opportunities that new IT can offer [16]. Leadership plays an integral role in the successful integration of ICT-technologies, as it promotes positive policies and a sense of readiness, while also easing resistance to change [17]. Learning is necessary for organisations [18], and mobile technologies have increased in the education sector [19].

Innovative culture builds on behavioral and cognitive change, where organizational learning can help maintain competiveness [20]. Change is naturally resisted in organisations, but the proper implementation of ICT, with open communication channels and enhanced information flows assist help overcome this resistance [21]. Flexible IT environments ease the integration of disparate and distributed systems, thus allowing them to control their outside environments more effectively [17]. Today, learners increasingly rely on ICT [22]. ICT can enhance learning and flows of knowledge in organizations [23]. Learners rely increasingly on ICT [22], whereby ICT-training promotes knowledge transfers, enhancing the ICT-skills of organization members [24]. Ideal contextual conditions that drive and optimize the use and organizational Knowledge Management practices highlights how managers need to design and implement relevant tools and practices, which in turn defines corporate culture [25].

2.2 Network Co-creation

Innovation in networks is based on developing new knowledge that drives growth and success [26; 27]. Creating knowledge for innovation calls for collaboration between research, business and public partners [28] on multiple layers, for example, involving agents and co-creating futures and policies [29]. Partners that collaborate in research and network projects have opportunities to generate new knowledge and skills that result in innovation [30].

Co-creation involves objectives, arenas, collaborators, tools, processes, and contracts [28]. Deep engagement of actors increases benefit across all stages of the innovation process [31], and co-creation in projects calls for collaboration and a common problem. Indeed, innovation networks promote open communication working towards co-creation of knowledge and eliciting stakeholder engagement throughout the project – processes which take time and effort [32]. Co-creation of knowledge occurs in physical and digital environments – singly or in combination [28]. Vos, Schoemaker and Luoma-aho [33] noted that when actors meet in physical or digital spaces to address and discuss issues that are relevant to them their communication takes place in 'Issue Arenas'. These are competitive spaces, where actors may have common agendas, but also have their own interests [34].

2.3 Societal Impact of Cyber Security

De Jong et al. [35] highlighted that societal impacts can be understood through productive interactions and 1) as a product, 2) as knowledge use, and 3) as societal benefits. Societal impacts as a product refers to knowledge having potential societal value that may be used by societal audiences, and embodied as a product (or service, information, tool, instrument, method, or model) [36]. Societal impacts as knowledge use can be seen as interaction processes between societal stakeholders, which result in the adoption of knowledge, which may be facilitated by a product [37]. Societal benefits can affect the use of innovation research results, whereby the focus can be on policy, professional or business practices, or impacts on culture, media and community (e.g. jobs, education, community formation, network building, trust) [38].

The internet and connected technology platforms have elicited the increase of cyber influence activity, where cybercrime, behaviour and actions target security and privacy on personal, corporate and national levels [39]. Cyber-attacks could even lead to environmental damage that can have a detrimental effect on the stability of society [40]. The ramifications of cybercrime go beyond the consequences inflicted by cyber-attacks themselves, whereby the functioning of economies could be impacted incurring significant costs [41].

Personal data is increasingly harvested and sold, wherein a key safeguard from cyber influence and harm is determined by maintaining an explicit awareness of what is real and fake. Technology can help detect and support awareness of personal privacy or national security harm related to identity

data and influence of their behaviour [39]. Economic and societal developments have become increasingly reliant on digitalization and ICT, which adds to the need for Cyber Security to protect these benefits [42]. Defending infrastructure from cyberattacks requires protecting information, network availability, and the global information grid, while safeguarding the citizens' lives and property, and preserving ecosystems and ecosystem services [40]. Effective, economic impact assessments require systematically collecting accurate reliable information, which can based on a framework of pre-set factors and indicators that provide better data on the agent-level costs of cybercrime and the respective social impacts as a means of supporting decisions on cyber security investments [41].

Bradshaw [43] noted that society may be aware of most emerging technologies and with the concept of disruption but may fail to understand the impacts that these innovations can have on society and the lives of its citizens. Tarafdar, Gupta, & Turel [44] denoted this as the 'dark side' of IT – a phenomenon that has the potential to violate the wellbeing of individuals, organizations and societies; is has therefore been proposed that policy makers should prepare for an upcoming technology-driven disruption of society [43].

2.4 Societal Impact Assessment

Impact assessment can be facilitated through organizational learning and stakeholder engagement approached, in turn making social learning outcomes visible [45]. Sánchez and Mitchell categorized group learning outcomes as: 1) acquisition of knowledge and skills, 2) developing new behaviors and 3) developing sustainability-oriented norms and values - wherein outcomes may be achieved using a 'learning organization approach', including education, training, experiential learning, learning through participation and social learning.

Henriksson et al. [30] furthermore highlighted the need for good practices for exploiting and disseminating innovation and research results. They proposed a framework of documentation when evaluating research impacts with quality dimensions (clarity, environment orientations, consistency, responsiveness and effectiveness) [46], and systematic documentation activities (e.g. quarterly dissemination and progress evaluation, exposure across targeted media audiences, two-way information transfer, commitment of project partners to project processes) [30]. Likewise, interactions can be understood through cycles of input, throughput, and output communication [47], and in the context of innovation projects, communication activities follow the elements of complexity in cyclical ways [48]. There are relevant studies that look at technical elements e.g. [49], [50], [51], but understanding the human element can broaden potential frameworks to evaluate the impacts of the work in innovation projects. According to e.g. Vos et al. [33] measurement processes need "strong commitment and an open culture of learning" (p. 66), and they find that in sensitive matters outcomes may be difficult to compare, so it "would be recommended to supplement self-assessment with other measures such as external assessment" (p. 66). Aaltola & Ruoslahti [45] noted that development of professional expertise must comply with network complexity and technological innovations: "Beyond relevant Societal Impact Assessment processes, complex network reality requires people who are committed on both organizational and individual levels to learn and adopt the knowledge, skills and competences required by the network co-creation and communities that there are involved in." (p. 3/14)

3 Method

This research is part of a series of actions and studies that together form the Societal Impact Assessment aspect of the ECHO project. This work serves as a qualitative pilot study to evaluate the usefulness of employing the Product/ Knowledge/ Benefit Societal Impact framework. This framework represents one initial phase within a larger continuum of separate works toward the development of appropriate quantitative methodology. This will be used to collect and analyse later quantitative data in selected case studies.

The current study serves as an integral building block in the development of the Societal Impact Assessment Toolkit. The data collection method for this pilot study mainly involved qualitative participatory observation [52]. This participatory observation aspect was based on a co-creative expert workshop (September 2020) wherein the societal impacts of five of the six ECHO assets were discussed. A total of 14 participants - composed of technology experts (i.e. computer engineers, project managers, software developers, programmers, computer science academics) - attended a two-hour hackathon workshop. The session used a qualitative 'think-tank' approach and was leveraged virtually by a moderator with a background in societal impact

studies. The technology experts were randomly allocated to five colour-coded teams and tasked to determine the greatest societal impacts which could be realised by assets which are currently in the process of being developed by the ECHO consortium.

Qualitative data aligning to each of the assets was assessed by means of thematic analysis, where a framework combining the ECHO assets and three forms of societal impact [35]. All EHCO assets were included in the hackathon session, however the E-MAF was not evaluated due to limited number of participants (n = 14); additionally their primary expertise and effort in the project were directed towards the other assets. This was not ideal, but as the purpose of this study was to serve as a qualitative pilot study to guide further quantitative methodology development and choices in the project task, this gap was deemed acceptable. Identifying societal impacts of the ECHO assets as product as knowledge use, and as benefits aid in formulating appropriate questions to in the next step devise and validate a quantitative questionnaire that can be widely used to collect a wide range of quantitative survey data to gain understanding of the human factors of societal impacts of cyber security within different European organisations.

4 Results

The workshop participants discussed how they perceived the societal impacts of five of six ECHO assets within the timeframe of five to ten years. Results are based on workshop notes provided by the participants.

4.1 ECHO Governance Model (E-GCS)

Product: The model of the E-GCS has the potential to speed up the development and exploitation of new cybersecurity products and services. New, more flexible employment models (e.g. self-employment) can potentially engage people in multiple CNOs and/or in virtual organizations.

Knowledge use: Each member will have access to advanced knowledge. This may enable them to better protect themselves, as well as to strengthen the cybersecurity of supply chains (i.e. CyberShield). Better, harmonized business and security practices among CNO members increase trust among members and in the entire community. Higher levels of trust by the users and other potential customers will facilitate the exploitation of the capacities of the CNO. Enhancing coordination, competencies within CNO may lead to federative responses to incident drills and thus, build resilience of the network, which is supported by faster co-generation of knowledge.

Societal benefits: Facilitated reduction of the cyber security debts that organizations have accumulated, increasingly during the COVID-19 crisis, will make organizations more viable and also more attractive as a workplaces.

4.2 ECHO Cyber Skills Framework and Training Curriculum (E-CSF)

Product: ECHO training programs may include university programs and courses, professional courses, and training programs, which actively use the other ECHO products (e.g. E-FCR, E-EWS). All these programs will, in their part, promote skills development, not only for ICT professionals, as the E-CSF helps design and create programs for people with different proficiency levels.

Knowledge use: By promoting practical learning experiences, the E-CSF can help achieve faster gaining of relevant cyber and e-skills. Promoting cyber-security knowledge and skills in all socio-economic domains will help limit the impacts of cyber-attacks. The E-CSF cyber-skills framework can support employers fill competence gaps, of both their experts and employees. Also, E-CSF can assist to hire experts with the appropriate skill set.

Societal benefits: The impacts of cyber-attacks can be limited, with increased cyber and e-skills. Education providers will have the possibility to also consider the market demand of competences to comply their programs with these needs. The ECHO approach in the design of training programs and assessment methodology may assist in this. EU-wide communication on threats, vulnerabilities, attacks, experiences, and knowledge exchange build common understanding that in turn may significantly improve the European cyber landscape and networks (e.g. ENISA, ECSO, EU Digital initiatives).

4.3 ECHO Security Certification Scheme (E-CCS)

Product: E-CCS will create reference framework that includes sector specific models from general certification schemes to mapping of standards. Product oriented cybersecurity certification schemes to support sector specific and inter-sector security requirements.

Knowledge use: The created E-CCS network can spread knowledge of certification, while also supporting high-level certification (e.g. ENISA Cyber Security Act). Increased knowledge of risks and potential solutions help increase users' trust in digital products by aiding in identifying relevant

risks. This, in turn helps build ability and capacity on all management levels to mitigate risks.

Societal benefits: E-CCS can help create inter-sector reference points. Product oriented cybersecurity certification schemes can support sector specific and inter-sector security requirements based digital single market that may limits duplication and fragmentation of the cybersecurity market, and common cybersecurity evaluation methods, accepted throughout Europe.

4.4 ECHO Federated Cyber Range (E-FCR)

Product: The multipurpose E-FCR services virtualization environment provides safe hands-on cyber skills development, realistic simulation for improved system assurance and development, and security test and certification evaluation.

Knowledge use: Added simulation elements and hands-on experiences, which cyber ranges provide, can lead to a wider diffusion of cyber security training, which could be introduced even much earlier in European school systems. General refinements of techniques and technologies help businesses cope better with competition. E-FCR services will provide organizations, be they academic, governmental, SME or large enterprise, easy and cheap access to a wide selection of cyber range services.

Societal benefits: Easy, inexpensive access to cyber range services may promote a general growth of the cyber range market, and help build general awareness of the possibilities of cyber ranges, which in turn can benefit the entire society in increased capacity to identify and mitigate cyber-security risks.

4.5 ECHO Early Warning System (E-EWS)

Product: E-EWS will enable national authorities and government agencies use the E-EWS to share information, identify cyber security threats and create mitigation tools and products, and even add additional functionalities to EWS. The E-EWS product can be used for education and procedural purposes.

Knowledge use: Knowledge use can best be promoted by sharing information. Increased knowledge and awareness of cyber security issues lead to better resilience of the community. E-EWS help national authorities (e.g. police) support local communities' fights against e.g. mass-phishing campaigns.

Societal benefits: Identifying successful mitigation techniques bring wider societal benefits. E-EWS (as a product, knowledge use and societal impacts) provide benefits for the wider community and can be used by computer emergency response teams (CERT) for incident notification according to ENISA Guidelines on notification of Operators of Essential Services incidents and NIS Directive.

5 Conclusions

The Societal Impact Assessment aspect of the ECHO project aims to introduce a quicker analysis for SIA and e-skills as well as an Assessment Methodology for SIA and e-skills, while referring to traditional effort-intensive qualitative methodology applied for SIA in preceding work and projects. This study serves as one of many that create a practical, but rigorous and relevant line of study that combined provide a basis for the deliverables of this project task.

For one, this is a qualitative pilot study that does not attempt to show percentage differences or draw quantitative conclusions demonstrates that this approach can provide relevant results. The study already shows that impacts can be structured according to the framework of ECHO assets [10] and three categories of societal impact [35], as seen in Table 2.

Table 2. Results structured according to the framework of analysis

	Product	**Knowledge use**	**Benefit to society**
E-GCS *ECHO Governance Model*	Faster development of cybersecurity products and services Faster exploitation of cybersecurity products and services New, more flexible employment models	Access to advanced knowledge Cybersecurity of supply chains More harmonized business and security practices Federative responses build resilience	Reduced organizational cyber security debt Organizations more attractive as a workplaces
E-CSF	Cyber security programs,	Promote cyber and e-	Limit impacts of cyber-

Cyber skills Framework	courses and training For different proficiency levels	skills development Organizations fill competence gaps	attacks Competence demand on market visible Builds common understanding
E-CCS *Security Certification Scheme*	Product oriented cybersecurity certification scheme Reference framework Sector specific models	Knowledge of certification High-level certification Knowledge of risks Knowledge of potential solutions	Inter-sector reference points Digital single market Common cybersecurity evaluation methods Acceptance throughout Europe
E-FCR *Federated Cyber Range*	Virtualization environment Realistic simulations	Access to cyber range services Wider cyber security training training even much earlier in European school systems	General growth of the cyber range market Build awareness Increased capacity to identify and mitigate cyber-security risks
E-EWS *Early Warning System*	Early warning system Incident notification for national authorities for computer emergency response teams (CERT)	Share information Identify cyber security threats Create mitigation tools and products	Support fights against cybercrime incidents Identify successful mitigation techniques

The workshop results show that ECHO is expected to have positive impacts on society, namely in improved network collaboration and information sharing. These were also identified as important aspects in the literature review [32; 28; 33]. The increased information sharing finding has the potential to increase overall cyber-security, as discussed in literature [39; 40; 41]. However, one shortcoming in these final conclusions is that they apply to this case, and cannot be widely generalized. To achieve this more study with a rigorous quantitative approach will be needed, and is recommended.

It is noteworthy, that all identified impacts can be rated as positive. Self-assessment can be complemented with external assessment measures, which highlights the need for such SIA methodology that encompasses rigour and relevance to provide practical and objective results. As Aaltola and Ruoslahti [45] posited, the path of development will look for ways to account for elements of complexity [48], working within the process [47] to understand SIA in the context of, not only individual ECHO assets, but also of the entire project. Further studies are recommended to incorporate societal impacts with cyber and e-skills. The matrix introduced by Aaltola and Ruoslahti [45] could be developed further and refined to include actual project key performance indicators (KPI). Relevant questions can then be developed based on these KPIs to provide a basis for both qualitative and quantitative inquiry.

Overall, this pilot study shows that the chosen methodology path is worth pursuing further. Societal impact can be examined as three elements (product, knowledge use, societal benefit) and through the lens of the ECHO assets. This pilot study serves as an initial qualitative step to validate the premise of this path to design and select practical, rigorous and relevant quantitative methodology to further the understanding of societal impact assessment in relation to the ECHO project assets, cyber and e-skills and their training in the same framework.

Proposed next studies are recommended to understand societal impacts of cyber security. The continuum of study will next focus on developing and validating a generalizable questionnaire of some 60 to 80 questions to assess societal impacts of cyber security. Once this questionnaire becomes answered by more than 100 respondents, quantitative validation methodology can be then used to identify the most relevant questions to provide a shorter 10 to 15 question survey. Furthermore, a gap assessment of relevant ICT / e-skills is needed to identify training and recruitment needs to better prepare against threats against cyber security. The contribution of this study is that it

starts a continuum of study to develop appropriately validated questionnaire based survey methodology that can provide understanding of the societal impacts of cyber security. This type of novel methodology approaches are needed. They contribute to both practice with very practical ways to assess impacts and skills. The contribution to theory is the possibility to collect sets of relevant quantitative data to deepen our understanding of societal impacts and relevant skills.

References:

[1] 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

[2] 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)

[3] 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

[4] Wilson C 2014 Cyber threats to critical information infrastructure *Cyberterrorism* (Springer New York NY) pp 123-136

[5] Morgan S (2019 Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021 *Cybercrime Magazine* June 10 2019

[6] Wadhwani P and Kasnale S 2020 *Cybersecurity Market Size By Product Type (Identity, Authentication and Access Management (IAAM)* (GMI3078).

[7] The Business Research Company 2020 (https://www.thebusinessresearchcompany.com/)

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

[9] 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-content/EN/ALL/?uri=CELEX:52017JC0450, accessed February 8 2021)

[10] ECHO network 2020 *ECHO network web-page* (https://echonetwork.eu/, accessed November 4 2020).

[11] Ruoslahti H and Trent A 2020 Organizational Learning in the Academic Literature – Systematic Literature Review *Information & Security: An International Journal* 46 no 1 pp 65-78

[12] 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

[13] 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

[14] Hortovanyi L and Ferincz A 2015 The impact of ICT on learning on-the-job *The Learning Organization* 22(1) pp 2-13.

[15] 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) pp 33-56

[16] 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) p 521.

[17] 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.

[18] 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

[19] 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).

[20] Cerne M, Jaklic M, Skerlavaj M, Aydinlik A Ü and Polat D D 2012 Organizational learning culture and innovativeness in Turkish firms *Journal of Management and Organization*

18(2) pp 193-219
[21] Yau H K and Cheng, A.L.F. (2010). "Influence of Organizational Defensive Actions on the Learning of Information and Communication Technology: An Attitude Study in Hong Kong". International Journal of Management, 27(3), pp. 459-469,579.
[22] Salleh K, Chong S C, Syed Ahmad S N and Syed Ikhsan S O S 2012 Learning and knowledge transfer performance among public sector accountants: an empirical survey *Knowledge Management Research & Practice* 10(2) pp 164-174
[23] Zhao F and Kemp L 2013 Exploring individual, social and organisational effects on Web 2.0-based workplace learning: a research agenda for a systematic approach *Association for Learning Technology Journal. Research in Learning Technology* 21
[24] Saleh M and Abel M 2018 System of Information Systems to support learners (a case study at the University of Technology of Compiègne) *Behaviour & Information Technology* 37(10-11) pp 1097-1110
[25] Perez-Soltero A, Leon Moreno F J, Barcelo-Valenzuela M and Lino Gamiño J A 2017 An Approach Based on Knowledge Management for the Use of ICTs in Mexican SMEs *IUP Journal of Knowledge Management* 15(4) pp 7-23
[26] Dandonoli P 2013 Open innovation as a new paradigm for global collaborations in health *Globalization and Health* vol 9 (1) 1-5
[27] 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 3 285-303
[28] Bhalla G 2014 How to plan and manage a project to co-create value with stakeholders *Strategy & Leadership* 42 (2) 2014 pp 19-25
[29] Accordino F 2013 The Futurium – a Foresight Platform for Evidence-Based and Participatory Policymaking *Philosophy & Technology* 26 (3) pp 321-332
[30] Henriksson K, Ruoslahti H and Hyttinen K 2018 Opportunities for strategic public relations - evaluation of international research and innovation project dissemination *Public Relations and the Power of Creativity, Advances in Public Relations and Communication Management*, Bowman, S, Crookes A., Romenti S and Ihlen Ø (eds.) volume 3 (Emerald Publishing Limited) pp 197 – 214
[31] DeFillippi R and Roser T 2014 Aligning the co-creation project portfolio with company strategy *Strategy & Leadership* 42 (1) 2014 (Emerald Group Publishing Limited) pp 30-36
[32] Ruoslahti H 2018 Co-creation of Knowledge for Innovation Requires Multi-Stakeholder Public Relations *Public Relations and the Power of Creativity, Advances in Public Relations and Communication Management* eds Bowman, S, Crookes A., Romenti S and Ihlen Ø volume 3 (Emerald Publishing Limited) pp 115-133
[33] Vos M, Schoemaker H and Luoma-aho V L 2014 Setting the agenda for research on issue arenas *Corporate Communications: An International Journal* 19 (2) 2014 (Emerald Group Publishing Limited) pp 200-215
[34] Vos M 2018 Issue Arenas *The International Encyclopedia of Strategic Communication (IESC)* eds Heath R and Johansen W (Whiley Blackwell, Malden MA)
[35] 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
[36] 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)
[37] Castro Martínez E, Molas Gallart J and Fernández de Lucio I 2008 *Knowledge transfer in the Human and Social Sciences: the importance of informal relationships and its organizational consequences*
[38] 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
[39] 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. IEEE)
[40] Kallberg J and Burk R A 2014 Failed Cyberdefense: The Environmental Consequences of Hostile Acts *Military Review* 94(3) p 22
[41] 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

[42] 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)

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

[44] 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

[45] Aaltola K and Ruoslahti H 2020 Societal Impact Assessment of a Cyber Security Network Project *Information & Security: An International Journal* 46 (1) pp 53-64

[46] Palttala P and Vos M 2012 Quality indicators for crisis communication to support emergency management by public authorities *Journal of Contingencies and Crisis Management* 20 (1) pp 39-51

[47] Vos M and Schoemaker H 2004 *Accountability of Communication Management, A Balanced Scorecard for Communication Quality* (Lemma Publishers, Utrecht)

[48] Ruoslahti H 2020 Complexity in project co-creation of knowledge for innovation *Journal of Innovation & Knowledge* (https://doi.org/10.1016/j.jik.2019.12.004)

[49] He Y, Ou L, Pu X, Li Y & Zhao Y 2019 E-commerce Network Security Protection Technology based on Mixed Data Encryption Strategy, International journal of Circuits, Systems and Signal processing, Volume 13, pp. 727-731.

[50] Patel C and Doshi N 2019 Cryptanalysis and Improvement of Barman et al.'s Secure Remote User Authentication Scheme, International journal of Circuits, Systems and Signal processing, Volume 13, pp. 604-610.

[51] Yu L, Guo Y and Jiang M, A 2019 Formal Method of Secrecy and Authentication Analysis for Ad-hoc Secure Routing Protocol, International journal of Circuits, Systems and Signal processing, Volume 13, pp. 320-327.

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