Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Ruoslahti, Coburn, Trent, and Tikanmäki,
Connections QJ 20, no. 2 (2021): 33-45
https://doi.org/10.11610/Connections.20.2.04

Research Article

Cyber Skills Gaps – A Systematic Review of the Academic Literature

Harri Ruoslahti,[1] Janel Coburn,[1] Amir Trent,[1] and Ilkka Tikanmäki [1,2]

[1] *Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland, http://www.laurea.fi/en*

[2] *Department of Warfare, National Defence University, Helsinki, Finland, https://maanpuolustuskorkeakoulu.fi/en*

Abstract: This literature review is part of research on the roles of and training for e-skills in modern society, specifically, the role of cyber skills. This article explores how the academic literature discusses cyber skills and identifies e-skills that can be determined as necessary for the functioning of society today. First, the introduction provides an explanation of the overall impact of cyber skills in our modern-day society. Next, the body presents the method used to conduct the review and a concise summary of the findings to answer our research questions. Finally, based on the research findings, the conclusions address the feasibility, impact, strengths, weaknesses, and possible ethical concerns.

Keywords: society, cybersecurity, cyber training, e-learning, cyber skills.

Introduction

The use of computers and other digital technology is a daily reality for over half of the global population and substantially more in modern European society. Of the roughly 7.8 billion people inhabiting the planet as of March 2020,[1] an

[1] Joseph Chamie, "World Population 2020: Overview," *Yale Global Online*, February 11, 2020, accessed April 12, 2020, https://yaleglobal.yale.edu/content/world-population-2020-overview.

estimated 59% are internet users and, as of 2019, 49% of those users have computers in their homes.[2]

Looking at the numbers above, it is logical to assume that a set of e-skills have become a prerequisite to functioning in society today. Therefore, the purpose of this literature review was to understand how cyber skills relate to e-skills and specifically to identify gaps and cyber skills that meet these gaps as they are discussed in the academic literature.

Project ECHO[3] (European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations), which started in 2019, aims at strengthening proactive cybersecurity in the European Union via a networked approach of effective and efficient multi-sector collaboration. This study adds to the body of knowledge, which the project cumulates, identifying how training for cyber skills is discussed in the academic literature and how they may relate to the broader spectrum of e-skills and the respective training can help design practical measures to identify and train focused cyber skills as part of a more general range of e-skills. In planning this study, we examined e-skills as skills needed to function in today's digital world, i.e., physically operate computers and smart devices and efficiently use the programs, applications, and digital information.

The cyber skills framework developed within the ECHO project represents an approach to describe the cyber skills requirements used to create the training curricula to equip cybersecurity professionals with the needed expertise to address the identified sectoral, transversal, and multi-sector cybersecurity challenges.[4] In addition, defining specific cybersecurity skills and related curricula for all levels of staff could fix the lack of awareness limiting responsivity to attacks. As described in ECHO research, cyber curricula and skills would help the healthcare and other sectors make a considerable step towards an entirely new level of cybersecurity.[5]

According to Chamie,[6] modern society has evolved into a technology-driven world due to the emergence of the Internet. The Internet has modified every aspect of social dynamics, from how business is being conducted (transforming traditional companies into digital-oriented firms) to how learning is being facilitated (e.g., with e-learning platforms) and how people interact with each other

---

2 Statista, "Share of Households with a Computer at Home Worldwide from 2005 to 2019," March 2, 2020, accessed April 11, 2020, https://www.statista.com/statistics/748551/worldwide-households-with-computer.

3 European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Grant Agreement Number: 830943 – ECHO – H2020-SU-ICT-2018-2020/H2020-SU-ICT-2018-2 (2019).

4 European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 121.

5 European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 64.

6 Chamie, "World Population 2020."

(thorough social networking platforms). With the advances in information and communications technology (ICT) tools, such as handheld mobile devices that provide constant and instant access to the Internet, people are more connected to ICT than ever before. ICT is essentially an integral component of our everyday lives. Besides the many benefits of utilizing the Internet and other ICT technology, there are unfortunately also threats, e.g., by cyber attackers who, with malicious intent, look to exploit vulnerabilities within these ICT applications. In order to delve into the significance behind developing cyber skills, this literature review focuses on cyber training and cyber skills development in relevant articles. The purpose of this review is to extend upon current knowledge regarding ICT training. To put this into perspective, the research questions of this study are:

RQ1: How does the academic literature discuss cyber skills gaps?

RQ2: What measures does the academic literature suggest in filling these gaps?

Methods

The main method used in this research is a systematic literature review. This is a qualitative study, and the main reason behind performing this systematic modern literature review is to identify the knowledge gaps of modern society pertaining to cyber skills to bring new insights to the field of e-skills development for further investigation.[7]

Qualitative Research Design

According to Kitchenham,[8] the systematic literature review is a thorough process that can help present evidence displaying the effects of certain events described in research and could not be conveyed in traditional non-systematic literature reviews. Systematic literature reviews may also be more extensive than regular ones. To perform this literature review, an academic search was conducted to find answers to the research questions. This study was conducted in a series of four steps: search, selection criteria, DET (data extraction table) analysis, and writing of the findings and conclusions.

Search

The search for articles was performed in March 2020. The search was conducted using the scientific databases ProQuest Central and EBSCO Host. The combination of “cyber security training” and “e-skills training” was used as search parameters in a Boolean keyword search. The period for the search spanned literature published within the ten years of 2010-2020.

---

7 Barbara Kitchenham, “Procedures for Performing Systematic Reviews,” Joint Technical Report TR/SE-0401 (Keele, UK: Keele University, 2004): 1-26, https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

8 Kitchenham, “Procedures for Performing Systematic Reviews.”

The ProQuest Central database search returned a total of 67 peer-reviewed articles, and the EBSCO Host database search returned two additional peer-reviewed articles. A final sample was selected for further analysis by applying inclusion criteria to the 67 articles in the initial keyword search. The inclusion criteria applied to the original 69 papers are: title or abstract includes themes related to cyber or e-skills training in the workforce and cyber or e-skills training in higher education. Applying the inclusion criteria rendered a final sample of 21 peer-reviewed articles (Table 1), which were all read thoroughly for analysis.

Table 1. Steps of Search and Resulting Numbers of Academic Papers.

Search Steps	Papers in Sample
Initial search results from ProQuest Central and EBSCO Host	69
After applying the Inclusion Criteria	21

The analysis of the final sample was done by extracting relevant pieces of information to a data extraction table (DET) based on the research questions. The next section discusses the findings from the sample of 21 articles.

Findings

Focus on Cyber Skills

The results indicate that cybersecurity is a significant concern in modern society. As new technologies with network capacity are being developed in connection with critical infrastructures and everyday activity, cyber devices are becoming vulnerable to cyberattacks by malicious actors. Spanning from identity theft to cyberbullying, these attacks can significantly influence financial, economic, and social systems. The large percentage of articles that did not meet the inclusion criteria indicates that many authors have a rather technological or risk-related focus on cybersecurity.

The articles included in the final sample indicate that most people who have access to ICT devices are at risk. People are either not sufficiently knowledgeable in cybersecurity or fail to practice proper cybersecurity measures. Challenges regarding cybersecurity vary depending on the age of the audience. Younger generations are more susceptible to cyber-attacks for several reasons: not practicing security measures, over-reliance on the security on their personal devices, lack of familiarity with new technologies centered around social media, or being most active in online shopping. Oversharing personal information in social networking sites or sites that third parties can harvest also contributes to the increased cybersecurity risk.

Overall, it is noteworthy that e-skills had significantly fewer mentions than cyber-related skills. Cybersecurity-related skills in the workplace and professional work are at the forefront of the discussions. Seventeen out of 21 peer-

reviewed articles addressed cybersecurity skills, cybersecurity training, or information/network security-related items. In fact, the search term "e-skills" produced only one result, and the other three remaining articles were found based on the keyword "e-learning." Based on these facts, one initial finding of the literature review is that the academic publications much more often discuss current cybersecurity threats, lack of cyber-related training and qualifications to deal with modern cyber threats, and new ways to provide training addressing cybersecurity threats.

The analysis of the data from the 21 sourced articles regarding e- and cyber skills found four major thematic categories.

1. General Cybersecurity: eight articles discuss the need and applications of cybersecurity training, awareness, and literacy.
2. Cybersecurity Training and Education: seven articles discuss the need for cyber education among certain academic programs, recommend cybersecurity training and education methods, and look at the differences between cyber education and cyber training. Cyber Ranges and Exercises emerged as a sub-category of Cybersecurity Training and Education. These articles discuss what these ranges and exercises are as training mechanisms and how they operate.
3. E-learning: five articles define e-learning, present barriers to e-learning, the need for ICT skills before e-learning can be accomplished, and discuss effective and specific, hands-on practical approaches for e-learning to be successful.
4. E-skills: only one primary article discusses an EU-wide need to increase ICT skills, why these e-skills are needed in everyday work and personal life, and how it affects the EU and global economy.

Eight out of the twenty-one articles make specific mentions of skills needed to operate professionally or in a personal capacity in everyday life or cybersecurity-related skills required to prevent malicious internet actors from achieving success. The one article that discusses specifically e-skills creates categories according to the level of e-skills needed to operate in daily work life. According to Singh,[9] these function categories are ICT practitioner skills, ICT user skills, and e-business skills.

General Cybersecurity

Table 2 below gives an overview of the eight papers that focus on cybersecurity training in general and their respective foci.

[9] Sumanjeet Singh, "Developing e-Skills for Competitiveness, Growth and Employment in the 21st Century: The European Perspective," *International Journal of Development Issues* (Emerald Group Publishing) 11, no. 1 (2012): 37-59, https://ideas.repec.org/a/eme/ijdipp/v11y2012i1p37-59.html.

Table 2. Articles that Relate to General Cybersecurity.

Article	Topic
Ricci et al. (2019)[10]	Survey results on adults and cybersecurity education
Clifton (2018)[11]	Increasing cybersecurity awareness in the hospice environment
Ghafir et al. (2018)[12]	Security threats to critical infrastructure: the human factor
Russell and Jackson (2018)[13]	Operating in the dark: Cyber decision-making from First Principles
Zăgan et al. (2018)[14]	Realities in the maritime domain regarding cybersecurity concept
Nikolova (2017)[15]	Best practice for cybersecurity capacity building in Bulgaria's public sector
Choi and Lee (2015)[16]	A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention
Rahim et al. (2015)[17]	A systematic review of approaches to assessing cybersecurity awareness

[10] Joseph Ricci, Frank Breitinger, and Ibrahim Baggili, "Survey Results on Adults and Cybersecurity Education," *Education and Information Technologies* 24 (2019): 231–249, https://doi.org/10.1007/s10639-018-9765-8.

[11] Tim Clifton, "P-236: Increasing Cyber Security Awareness in the Hospice Environment," *BMJ Supportive & Palliative Care* 8, no. 2 (2018): A94, https://dx.doi.org/10.1136/bmjspcare-2018-hospiceabs.261.

[12] Ibrahim Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," *The Journal of Supercomputing* 74 (2018): 4986-5002, https://doi.org/10.1007/s11227-018-2337-2.

[13] Scott Russell and Craig Jackson, "Operating in the Dark: Cyber Decision-Making from First Principles," *Journal of Information Warfare* 17, no. 1 (2018): 1-15, https://cacr.iu.edu/files/documents/Operating_in_the_dark.pdf.

[14] Remus Zăgan, Gabriel Raicu, Radu Hanzu-Pazara, and Stănică Enache, "Realities in Maritime Domain Regarding Cyber Security Concept," *Advanced Engineering Forum* 27 (April 2018): 221-228, https://doi.org/10.4028/www.scientific.net/AEF.27.221.

[15] Irena Nikolova, "Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector," *Information & Security: An International Journal* 38 (2017): 79-92, https://doi.org/10.11610/isij.3806.

[16] Kyong-Ho Choi and Donghwi Lee, "A Study on Strengthening Security Awareness Programs based on an RFID Access Control System for Inside Information Leakage Prevention," *Multimedia Tools and Applications* 74, no. 20 (2015): 8927–8937, https://doi.org/10.1007/s11042-013-1727-y.

[17] Noor Hayani Abd Rahim et al., "A Systematic Review of Approaches to Assessing Cybersecurity Awareness," *Kybernetes* 44, no. 4 (2015): 606-622, https://doi.org/10.1108/K-12-2014-0283.

According to Rahim et al.,[18] adults may commit risky online behavior, for example, accessing private e-mails on public Wi-Fi networks, clicking on unfamiliar links, or using the same passwords for multiple online accounts. In addition, seniors tend not to be as cyber-savvy as the younger generation and exhibit more trustworthiness, which may be exploited through phishing and social engineering attacks, thus exposing their vulnerability.

Cybersecurity Training and Education

Table 3 below lists the seven papers included in the final sample and their foci on cybersecurity training.

Table 3. Articles that Relate to Cybersecurity Training and Education.

Article	Topic
Yamin et al. (2020)[19]	Cyber ranges and security testbeds: scenarios, functions, tools, and architecture
Aaltola and Taitto (2019)[20]	Utilizing experiential and organizational learning theories to improve human performance in cyber training
Beuran et al. (2019)[21]	Supporting cybersecurity education and training via LMS integration: CyLMS
Raineri and Fudge (2019)[22]	Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs
Chapman et al. (2017)[23]	Can a network attack be simulated in an emulated environment for network security training?

[18] Rahim et al., "A Systematic Review of Approaches."

[19] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers and Security* 88 (January 2020), 101636, https://doi.org/10.1016/j.cose.2019.101636.

[20] Kirsi Aaltola and Petteri Taitto, "Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training," *Information & Security: An International Journal* 43, no. 2 (2019): 123-133. https://doi.org/10.11610/isij.4311.

[21] Razvan Beuran et al., "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS," *Education and Information Technologies* 24 (2019): 3619-3643, https://doi.org/10.1007/s10639-019-09942-y.

[22] Ellen M. Raineri and Tamara Fudge, "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs," *Journal of Higher Education Theory and Practice* 19, no. 4 (2019): 73-92, https://doi.org/10.33423/jhetp.v19i4.2203.

[23] Samuel Chapman et al., "Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?" *Journal of Sensor and Actuator Networks* 6, no. 16 (2017), https://doi.org/10.3390/jsan6030016.

Adams and Makramalla (2015)[24]	Cybersecurity skills training: an attacker-centric gamified approach
Lester (2010)[25]	A practical application of software security in an undergraduate software engineering course

Results show that cybersecurity, in most cases, becomes compromised due to human errors and inadequate cybersecurity awareness and skills. With cybersecurity becoming a pressing issue in modern society by affecting businesses, personal life, and critical infrastructures, there is a growing need for proficiently cyber-trained personnel to protect these systems.

Topham and colleagues[26] reason that the organizations aiming to prepare adequately to withstand threats that can compromise their security and continuity of operations must secure every critical element of their infrastructure. The foundation starts with users who, as results indicate, are often established as the weakest link due to not being educated in cyber threats concepts and not having the experience to mitigate cyber threats that may arise. Social engineering and phishing are the most common attacks end users usually encounter. With no prior relevant training in cybersecurity, these users can rarely distinguish between a legitimate request and a cyberattack. As a result, they may inadvertently leave their company network vulnerable to threat actors. The results raise the recommendation to invest in cybersecurity awareness programs and cyber training to deal with cyber threats. Ghafir et al.[27] see that a challenge in implementing cybersecurity training and education in organizations is knowing how to properly provide training that will effectively engage staff (who are not ICT personnel) to practice security awareness and develop their cyber skills. For ICT professionals, the challenge is to become more proficient in analyzing and managing the constantly evolving cyber threats.

Adams and Makramalla[28] note that the main obstacle affecting personnel from learning how to apply security measures and establish cybersecurity skills stems from the instruction they receive from cybersecurity education programs. Most of these programs teach security concepts in a traditional approach, where it may be challenging to retain the information or put it into practice. Instead, supplementing theoretical knowledge with experiential learning and interactive

[24] Mackenzie Adams and Maged Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," *Technology Innovation Management Review* 5, no. 1 (January 2015): 5-14, http://doi.org/10.22215/timreview/861.

[25] Cynthia Y. Lester, "A Practical Application of Software Security in an Undergraduate Software Engineering Course," *International Journal of Computer Science Issues* 7, no. 3 (May 2010): 1-9.

[26] Luke Topham et al., "Cyber Security Teaching and Learning Laboratories: A Survey," *Information & Security: An International Journal* 35, no. 1 (2016.): 51-80, https://doi.org/10.11610/isij.3503.

[27] Ghafir et al., "Security Threats to Critical Infrastructure."

[28] Adams and Makramalla, "Cybersecurity Skills Training."

training (e.g., games, puzzles, scenarios) for general employees could provide more practical hands-on training that looks at real situational threats (e.g., via cyber ranges). Cybersecurity training programs, run by the organizations' own ICT professionals, can effectively optimize the development of cybersecurity skills and security awareness in employees so that they can competently defend themselves and organizational assets against attacks.

According to Topham et al.,[29] practical training through network simulated exercises and interactive cyber lab training can be beneficial in developing relevant cyber skills for students learning cybersecurity training in higher education. This may make them desired by companies when they enter the workplace as cyber-savvy employees and even future cyber professionals with competencies to deal with current and future cyber threats as ICT technology continues to advance.

E-learning

Table 4 below provides an overview of the five papers that focus on e-learning. E-learning was seen as an essential asset for organizations to invest in to achieve optimal business and individual performance in all their activities centered around ICT technology. This entails the provision of e-learning programs that develop e-skills and education necessary to use modern ICT-based devices, networks, and systems efficiently.

One of the most popular methods for e-learning, mentioned by Annansingh and Bright,[30] is web-based e-learning, where resources are distributed through web-based platforms and are accessible on any computer system connected to the Internet. Some benefits associated with web e-learning are remote accessibility, being able to work on courses at any location and time, possibilities for interactive training by, for example, practical applications that focus on situational instances, as opposed to instructor-led training that uses lectures in teaching security concepts, and the ability to repeat previous courses to absorb the concepts more thoroughly. Lastly, information from web-based e-learning is better retained compared to traditional training.

As many benefits are exhibited through e-learning, one obstacle that presents a challenge of taking advantage of e-learning involves having essential ICT skills. Employees with limited ICT skills may not be able to digest the information adequately, compared to others more used to working with and skillful in ICT. Some barriers that were noted are the lack of adequate time to devote to e-learning, resistance to change regarding preference in training (contact instructor-led training vs. online training), and maintaining discipline while participating in longer e-learning courses. All these reasons may result in drop-outs as courses lengthen. Having prior negative experiences in e-learning courses may also hinder success.

[29] Topham et al., "Cyber Security Teaching and Learning Laboratories."

[30] Annansingh and Bright, "Exploring Barriers to Effective e-Learning."

Table 4. Articles that Relate to E-learning.

Article	Topic
Iqbal (2016)[31]	Design and emergence of a pedagogical online InfoSec Laboratory as an ensemble artefact
Topham et al. (2016)[32]	Cybersecurity teaching and learning laboratories: a survey
Hagen et al. (2011)[33]	The long-term effects of information security e-learning on organizational learning
Annansingh and Bright (2010)[34]	Exploring barriers to effective e-learning: Case study of DNPA
Anonymous (2010)[35]	E-learning at Dartmoor National Park Authority: How to minimize drop-out rates and resistance to future training programs

Annansingh and Bright[36] recommend that to deliver successful e-learning courses, consideration must be given to the needs of the e-learner. The success of e-learning programs is determined, on the one hand, on how the course is implemented and, on the other, on the recipient. The weaknesses of the e-learner may prevent the employee from participating and benefitting in e-training. Results indicate that creating incentives (e.g., promotion or increased salary) may better encourage employees to embrace e-learning training.

E-skills

As seen in Table 5 below, the final sample included only one paper that discusses the term e-skills.

[31] Sarfraz Iqbal, "Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact," *Journal of Information Systems Education* 27, no. 1 (2016.): 17-35, https://aisel.aisnet.org/jise/vol27/iss1/2.

[32] Topham et al., "Cyber Security Teaching and Learning Laboratories."

[33] Janne Hagen, Eirik Albrechtsen, and Stig Ole Johnsen, "The Long-term Effects of Information Security e-Learning on Organizational Learning," *Information Management & Computer Security* 19, no. 3 (2011): 140-154, https://doi.org/10.1108/09685221111153537.

[34] Fenio Annansingh and Ali Bright, "Exploring Barriers to Effective e-Learning: Case Study of DNPA," *Interactive Technology and Smart Education* 7, no. 1 (2010): 55-65, https://doi.org/10.1108/17415651011031653.

[35] Anonymous, "E-learning at Dartmoor National Park Authority: How to Minimize Drop-out Rates and Resistance to Future Training Programs," *Development and Learning in Organizations* 24, no. 6 (2010): 20-22, https://doi.org/10.1108/14777281011084720.

[36] Annansingh and Bright, "Exploring Barriers to Effective e-Learning."

As discussed by Singh,[37] the world develops into a more ICT-oriented society, and developing general ICT skills (e-skills) becomes necessary. Due to the prevalent influence ICT has on social and personal life, E-skills are essential in modern society. Investing in ICT / e-skills can provide many advantages, and cyber skills create the competence and possibilities to protect oneself against cyber threats.

Table 5. Articles that Relate to E-skills.

Article	Topic
Singh (2012)[38]	Developing e-skills for competitiveness, growth, and employment in the 21st century

Conclusions

The academic literature primarily discusses current cybersecurity issues, such as cyber threats, cyber-related training and qualifications, and training. It is suggested to invest in studies defining what e-skills, in addition to the necessary cybersecurity-related skills, are needed to operate in modern society effectively. Four major categories regarding e-skills emerge as results of this study. As seen in Table 6, these categories serve to understand the role of cyber and e-skills in modern society. It becomes apparent that users, be they private citizens, working professionals, or ICT / cyber experts, are a potential weak link regarding cyber issues. Thus, cyber skills are needed to protect people, organizations, and society against disruptive cyber incidents and malicious cyberattacks.

Cybersecurity awareness programs that accommodate all audiences with varying degrees of e-skills and cyber knowledge can help people invest more in cultivating cybersecurity culture, with proper online behavior and a mindset towards online protection. Furthermore, such a security awareness platform could be complemented by delivery methods that effectively address cybersecurity issues and topics related to cyber threats while simultaneously improving the understanding of cyberattacks. By implementing these countermeasures of cybersecurity awareness, people can become more inclined to embrace cybersecurity awareness and be prepared to practice security measures when connected online, facilitating safer behavior in cyberspace and positive societal impacts.

When users have difficulties distinguishing between legitimate requests and possible cyberattacks, there is a gap in providing relevant cybersecurity training. Therefore, investing in cybersecurity awareness programs and cyber training to deal with cyber threats should be organizations' priority.

[37] Singh, "Developing e-Skills for Competitiveness."

[38] Singh, "Developing e-Skills for Competitiveness."

Table 6. Main Findings.

Category	Main Findings
General Cybersecurity	• cyber devices vulnerable to cyberattacks • people are either not knowledgeable in cybersecurity or fail to practice cybersecurity measures
Cybersecurity Training and Education	• end-users often considered as the weakest link • recommendation to invest in cybersecurity awareness programs and cyber training • practical training through network simulated exercises and interactive cyber lab training can be beneficial
E-learning	• e-learning as an essential asset for organizations to invest in • benefits of web-based e-learning: remote accessibility, work at any location/time, interactive training possible
E-skills	• modern society has gradually become more technology driven • the development of e-skills training has become essential • e-skills pertain to activities of both business people and or casual users • benefits of developing e-skills are extensive on a personal level

As ICT has become a critical factor in establishing global competitiveness, growth, and innovation in Europe, it is necessary to invest in e-skills education and cybersecurity training in order to develop resilient societal, economic, and industrial systems. Governments and academic institutions could help various organizations address shortages in ICT competence in the workplace by facilitating cyber skills training courses and education in e-skills, thus continually cultivating growth and innovation in the European economies through ICT developments.

In addition, to incorporate effective cybersecurity and e-skills programs, educators should address the factors preventing users from investing in these programs. Instructors may tailor their pedagogical methods and systems in ways that best benefit end-users while optimizing the enhancement of their e-skills. As a result, the learner has an engaging experience within these programs and can use the new skills for personal improvement while contributing to society.

This study shows a general lack of established IT terms. There are "e-skills," "cyber skills," "computer skills," "ICT skills," and they all can mean different things to different authors. We recommend continued research to identify clear definitions for each of these terms.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

This work was supported by the ECHO project, which has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no. 830943. The European Commission-funded cyber pilot projects, such as the "European network of Cybersecurity centres and competence Hub for innovation and Operations" (ECHO), bring opportunities for researchers to conduct experiments and gather empirical data to study these aspects from different perspectives.

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

About the Authors

Harri Ruoslahti, PhD, is a Senior Lecturer in Security and Risk Management of the Laurea University of Applied Sciences. He also leads Laurea's team in the Horizon 2020 project "European network of Cybersecurity centres and competence Hub for innovation and Operations" (ECHO).
E-mail: harri.ruoslahti@laurea.fi

Janel Coburn worked as Research, Development, and Innovations Expert at Laurea University of Applied Sciences, where she contributed to several RDI projects, including the study of cyber skills in the ECHO project.

Amir Trent was a BSc student in Business Information Technology at Laurea University of Applied Sciences.

Ilkka Tikanmäki is a researcher in Security and Risk Management at the Laurea University of Applied Sciences and a doctoral student of Operational art and tactics at the Finnish National Defence University.