Information & Security

I. Tikanmäki & H. Ruoslahti
vol. 55, no. 3 (2024): 225-235
https://doi.org/10.11610/isij.5506

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Insights on Human Factors Enhancing Cybersecurity

Ilkka Tikanmäki [1,2] (✉) *and Harri Ruoslahti* [1]

[1] *Laurea University of Applied Sciences, Espoo, Finland, https://www.laurea.fi/en/*

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

ABSTRACT:

This study analyses reports on human factors published by the ECHO project. The project produced 110 publications throughout its duration. It aimed at strengthening technological sovereignty by centralising Europe's cybersecurity efforts and establishing a unified market for technical solutions through unique cybersecurity capabilities applicable to sectors such as healthcare, transport, education, research, energy, civil protection, and public and private organisations. The importance of human factors in cybersecurity is emphasised in this study, which analysed six academic articles which underlined innovation, excellence, and people. The study emphasises the importance of effective training, recruitment, and management in strengthening cyber security and resilience. The publications shed light on the competencies and skills necessary for robust cybersecurity training that contributes to Europe's cybersecurity ecosystem.

Enhancing cybersecurity awareness requires that all members of an organisation understand cybersecurity-related topics and issues. Organisations often seem to fail to recognise that the lack of understanding is a major security vulnerability in daily business operations. Increasing organisational awareness can reduce security breaches. The solution to this problem lies in the implementation of adequate training programs.

ARTICLE INFO:

RECEIVED: 13 AUG 2024
REVISED: 20 OCT 2024
ONLINE: 01 NOV 2024

KEYWORDS:

human factors, ECHO project, cybersecurity, resilience, training, skills, competencies, cybersecurity ecosystem

✉ E-mail: ilkka.tikanmaki@gmail.com

Introduction

This study is based on human factors publications of the European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) project,[1] including conference papers and journal articles. Innovation, excellence, and people were the primary objectives of the ECHO project, which aimed to centralise Europe's cybersecurity efforts. The ECHO project involved 30 partners from 14 European countries, spanning various sectors such as healthcare, transport, manufacturing, ICT, education, research, telecommunications, energy, space, defence, civil protection, and public and private organisations. Providing a single market for cybersecurity technical solutions and developing unique cybersecurity capabilities is part of strengthening Europe's technological sovereignty. The project resulted in 110 publications published in total. The ECHO project has several publications dedicated to human factors in cybersecurity.

Besides many benefits, ICT technologies face threats, as vulnerabilities in ICT applications and systems may become exploited in ways that require appropriate employee e-skills. The Allianz Risk Barometer ranked cyber incidents as the greatest risk threatening business continuity.[2] Hence, organisations of today face many challenges that require technical, situation awareness, and problem-solving-related e-skills from a wide spectrum of organisational actors.

Publications provide information on the competencies and skills necessary for effective cybersecurity training. The importance of human factors in cybersecurity is highlighted in these publications, which stress the need for proper training, recruitment, and management to enhance cybersecurity resilience. The ECHO project and other related publications emphasise the importance of human factors in improving cybersecurity resilience. The key contributions include user awareness and education, organisational culture, human-computer interaction, leadership, communication, and psychological and human factors.

The research question of this study is: How do human factors contribute to the enhancement of cybersecurity resilience as evidenced by the publications from the ECHO project?

The structure of this article is as follows: Section 2 covers the literature review, section 3 details the methodology, section 4 showcases the study's findings, and section 5 concludes by summarising the study findings.

Literature Review

The cybersecurity field is centred around the individuals involved, whether working directly on security measures or relying on secure infrastructure to complete their tasks. There are many standards and best practices dedicated to cybersecurity technologies and processes. To address the human element, individuals are typically classified as IT/cyber professionals or end-users who require training.[3] The focus of traditional information security is to safeguard data sources and the roles of individuals in security processes, while cyber security considers individuals to be either potential targets or participants in cyber-attacks.[4] Identity theft, fraud, stolen hardware, access rights violations, system

intrusion, and misuse of instant messengers are some consequences of cyber-attacks. The human interface is the target of semantic cyber-attacks, making them more serious than physical and syntactic cyber-attacks.[5] The importance of human performance in cybersecurity lies in the role played by human and organisational factors in reducing computer and information security (CIS) vulnerabilities.[6, 7] Citizens and professionals will be able to better prepare for threats and manage vulnerabilities and disruptions by improving their cybersecurity skills.[8] In many cases, human errors are caused by insufficient cybersecurity awareness and skills.[9]

Situational awareness (SA) is an important non-technical skill in human factors.[10] SA is the result of understanding meaning and anticipating future events based on perception.[11] In normal and emergencies, decision-making is influenced by experience or new information in assessing the situation, making a diagnosis, or choosing a course of action.[12] Cyber exercises are designed to teach problem-solving, decision-making, analytical skills, and SA. SA is considered essential for describing, measuring, and predicting human performance in cyber security. The process involves recognising, comprehending, and projecting the situation.[13, 14]

To adequately prepare for threats, organisations must secure all critical parts of their infrastructure. Cyber security awareness programs and cyber training are recommended for organisations to invest in to combat cyber threats. Users should not accidentally leave their corporate network open to threat actors.[15] Developing analysis and management skills in the constantly evolving cyber threats is a challenge for ICT professionals. Users are often unable to distinguish between legitimate requests and cyberattacks without proper cybersecurity training, with manipulation and phishing being the most common attacks that end users usually encounter.[16]

Success in everyday work life depends on the important social and organisational aspects that are often overlooked. Problem-solving, communication, and collaboration, among other non-technical knowledge, skills, and abilities (KSAs), can also be advantageous.[17] The requirement for cybersecurity professionals is to communicate technical information to non-technical people.[18] Professional development training and higher education programs for cybersecurity professionals should incorporate non-technical KSAs.[19]

Method

A case study is an empirical study exploring a current phenomenon within its real-life context.[20] Qualitative research is a process that relies on data.[21] Methods and knowledge are context-dependent, and rules do not dictate the data to be collected for studying a particular interest or problem. Methods cannot be determined using a set recipe or formula.[22]

Templier and Paré [23] outline a six-phase process for conducting a study: formulating the problem, defining the research objectives (research question), searching for existing literature, screening for inclusion, assessing quality, extracting data, interpreting the data, and writing a summary. Similarly, Leitner and co-authors [24] describe a six-stage process for conducting a literature review: selecting a topic, researching the literature, developing an argument, surveying the literature, critiquing the literature, and writing the review,[25] guidelines were used to ensure transparency in reporting during the systematic literature review conducted for this study.[26] The purpose of this review is to discover which human factors exist in the publications of the ECHO project. There were 110 publications on the ECHO web page. Publications were checked and reviewed in three phases. The first phase in finding relevant publications was based on their titles. The second phase involved reading the Abstracts based on relevant titles. Reading the complete text of the chosen publications was the third phase.

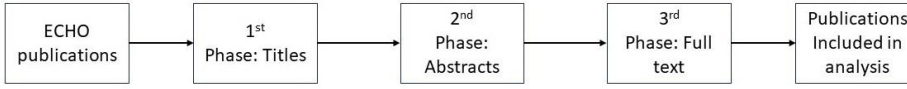

Figure 1: Review Process.

The initial phase involved checking the titles to exclude unrelated publications. Phase one was skipped due to the absence of keywords directly related to the topic in the titles. Inclusion criteria keywords in the abstract were chosen because they were deemed to appear in the abstract as important to the authors. The finding from this stage shows that most of these 110 articles are quite technical in nature. To identify relevant and non-relevant publications was done by reading the abstracts in the second phase. The entire texts were examined for analysis in the third phase and the final step included 11 publications for further analysis. All 11 publications were analysed, resulting in the selection of six publications focusing on human factors. The five excluded articles did not meet the criteria of human factors. This study analyses human factors in cybersecurity by collecting, grouping, and regrouping their studied features. This categorisation approach was used to conclude how human factors in cybersecurity can be influenced.

Results

The following table contains the final sample of six articles about Human Factors from ECHO publications used in this study.

De La Vallée and co-workers investigated how to raise awareness about cyber threats in the energy sector.[27] Security incidents in organisations and throughout the energy sector were found to be caused by a lack of understanding in multiple case studies. Social engineering and lack of awareness have the potential to lead to serious consequences that put entire systems at risk. In some organisations, data security practices are either outdated or not properly implemented. If this issue is not addressed, it could

Table 1. Articles selected from ECHO publications.

Authors	Publication Title	Publication channel
Almén, Hagström and Rajamäki (2022)	ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector	Journal Article
de La Vallée, Iosifidis and Mees (2022)	Cyber Red Teaming: Overview of Sly, an Orchestration Tool	Journal Article
Aaltola & Taitto (2019)	Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training	Journal Article
Frisk, Tikanmäki and Ruoslahti (2022)	Piloting the ECHO e-Skills and Training Toolkit	Journal Article
Varbanov (2022)	Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach	Journal Article
Mäses, Maennel and Brilingaité (2022)	Trends and Challenges for Balanced Scoring in Cybersecurity Exercises: A Case Study on the Example of Locked Shields	Journal Article

result in security breaches. Situational awareness is an important element that can be used to solve the critical problem of security incidents. Situational awareness refers to a person's understanding of the current situation and how their actions affect the situation. The level of understanding and awareness can be achieved by following an appropriate security policy within the organisation. The security policy must include good training for all employees and continuous development of cyber security.

Another publication of the authors focused on understanding the situation, the person's role in it, and the importance of exercises in developing competence.[28] Improving personnel's ability to respond appropriately and adequately to intrusions in a production context can be improved through practical exercises in the cyber domain that simulate realistic situations. The reports indicate that people are still perceived as the weakest link in the security chain. The solution requires a successful attack response and recovery, which is also a human achievement. Choosing the most appropriate actions in a complex dynamic context requires a lot of specific knowledge, skills, and abilities (KSA). Situational awareness (SA) is a theory that describes how individuals perceive and act on their surroundings. SA serves as a fundamental support for making appropriate decisions. The quality of SA is determined by how well an individual can use

their cognitive abilities. Schemas and mental models are formed by people who gain experience through education or exposure to different situations. Beginners' progression towards expertise is a result of integrating experience into mental models and using it sufficiently. It is common for individuals to ignore new environmental cues and instead adopt less adequate schemas. Realistic, complex, versatile, up-to-date, and representative of production situations are necessary for training scenarios. The training's effectiveness is enhanced by the integration of theoretical knowledge into exercises and the practical dimension.

Aaltola and Taitto [29] analysed current practices and reflected on aspects of human performance in cyber security training and practice. The human dimension of the organisation is undergoing a radical transformation due to new and emerging technologies like autonomous systems, machine learning, and artificial intelligence. Strategic changes have exposed new critical vulnerabilities, which affect human aspects, like social media-based election interference and disinformation campaigns. Cyber security training and exercises should take into account the unique features of cyber security skills. Learning, education, and training at the societal level have become more relevant by improving capabilities and human competencies in the cyber domain. The role of human behaviour and decision-making is crucial in cyber security. This reality should be replicated as closely as possible in education and training. The cyber field needs to be seen as a constructive process for developing human skills and competencies. It is necessary to acknowledge and utilise the skills that the learner has already acquired. The members of the organisation collaborate to build and construct the necessary knowledge, know-how, and expertise in a complex environment. The utilisation and conceptualisation of learning approaches could be enhanced in cyber security training, education, and exercises. Human performance could be better prepared, especially in skills such as decision-making. The authors recommend studying more human performance and human aspects in cyber education. Aspects of human-technology interaction could also be included in cyber training and exercises that improve human performance.

Frisk et al. in their article [30] argue that as a society and its organisations and systems are increasingly at risk, there is a greater need for highly skilled cyber-trained personnel. ICT applications and systems are vulnerable to threats, which require employees to possess appropriate electronic skills. Cyber accidents were assessed by Allianz's risk barometer as the most significant risk to business continuity in 2020. The challenges faced by today's organisations demand technical, situational awareness, and problem-solving skills from their employees. The purpose of the study was to test ECHO's E-skills and Training Toolkit methodology, which has the potential to identify e-skills that are relevant to cyber security. The purpose of this method is to evaluate educational gaps. The case is centred around the practical use and testing of the E-skills and Training Toolkit provided by the ECHO project. The focus of this toolkit is on cybersecurity e-skills, specifically technical, situational awareness, and problem-solving skills. Organisations can identify their key e-skills gaps understandably and systematically, as demonstrated by this pilot study. This suggests a structured way to

identify and address training, recruitment, and development that is based on needs. Identifying and prioritising technical skills related to situational awareness and problem-solving can be done systematically by users of the organisation. Organisations can focus on the training that their current staff needs and hire people to fill the gaps in their team/organisation's e-skills. Businesses can benefit from these insights in building their cyber defences.

Varbanov [31] argued that strong and sustainable cybersecurity practices can only be achieved using human capital. Well-structured, practical, and research-based information is necessary for the rapidly spreading digitisation in all sectors of society and the economy. Necessary tools for developing cybersecurity knowledge, skills, and competence are provided by research information to individuals, organisations, and industries. The ECHO project aims to identify gaps in personnel readiness using analytical and cyber-risk-based tools to execute tasks related to cyber defence, and practical learning tools to address these shortcomings. The approach proposed by Varbanov explores and develops general definitions of the skills and knowledge required for information and communication technology or cybersecurity professionals. It emphasises what these professionals must know and be able to implement, including cyber accident countermeasures and other necessary actions.

Mäses et al.[32] claim that building resilience against cyberattacks requires conducting cybersecurity exercises (CSXs) to enhance organisational awareness, test capabilities, identify strengths and weaknesses, and gain practical experience. The structure of these exercises often involves competitions or challenges, with gamification elements added to boost participant engagement and motivation. In developing organisations and communities, cybersecurity exercises (CSXs) are becoming more popular to improve cyber-resilience. Participants can experience a complex and realistic training environment through these exercises that simulate incident response situations. Cyber-attacks are divided into three sub-categories: web, network, and client-side. Threats related to the human factor are simulated in client-side attacks, which frequently take advantage of vulnerabilities in the user's browser or device to steal sensitive information or install malware.

Conclusions

The results from the analysed sample show that to increase cybersecurity awareness and relevant cybersecurity topics should be understood across the organisation. This can be a major issue in countering cyber security vulnerabilities in day-to-day business. However, based on the results, it is not emphasised enough by all companies and organisations. Increased awareness throughout the entire organisation will lead to a decrease in data security breaches and incidents. Having adequate training programs in organisations is the solution offered to this problem.

Human factors play a critical role in improving cybersecurity resilience, as highlighted by the ECHO project and other related publications. Key contributions are user awareness, education, organisational culture, human-computer

interaction, leadership, and communication, as well as psychological and social factors, as presented in Table 2.

Table 2. Key Contributions of Human Factors.

Contribution	Description
User awareness	Cybersecurity threats and best practices
User education	Cybersecurity threats and best practices
Organisational culture	Prioritise cyber security in daily activities
Human-computer interaction	User-friendly systems
Leadership	Cybersecurity measures understood
Communication	Cybersecurity measures communicated
Psychological	Understanding psychological dynamics
Social factors	Understanding social dynamics

The risk of human error, which often is a major cybersecurity vulnerability, can be significantly reduced by educating users about cybersecurity threats and best practices (Table 2). Employees should prioritise cyber security in their daily activities by promoting a security culture in organisations. This includes fostering an environment where it is encouraged and supported to report potential threats.

By designing user-friendly security systems and paying attention to human behaviour and cognitive limitations, compliance can be improved, and errors can be reduced. The creation of user interfaces that are intuitive and decrease the likelihood of mistakes is necessary. The implementation and maintenance of strong cyber security measures require effective management and clear communication strategies.

Managers are responsible for ensuring cybersecurity policies that are effectively communicated and understood by all employees. Identifying potential insider threats and mitigating them with targeted measures can be achieved by understanding the psychological and social dynamics of an organisation. By integrating these human factors into cybersecurity strategies, organisations can build more resilient systems that are better equipped to handle and recover from cyber threats.

Acknowledgements

Acknowledgement is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] ECHO project, "ECHO Network," Project summary, 2022, https://echonetwork.eu/.

[2] Allianz Commercial, "Allianz Risk Barometer: Identifying the Major Business Risks for 2024," Risk Barometer (Munich, Germany: Allianz Global Corporate & Specialty SE, 2024), https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf.

[3] ECSO, "Understanding European Cybersecurity HR Recruitment Processes," A collaboration between the European Cyber Security Organisation (ECSO) and the European Cybersecurity Competence Network Pilot projects (Brussels, Belgium: European Cyber Security Organization, 2021), https://echonetwork.eu/wp-content/uploads/2021/12/Report-on-EHR4CYBER-survey_ECSO-and-the-Pilots_v0.1_final.pdf.

[4] Rossouw von Solms and Johan van Niekerk, "From Information Security to Cyber Security," *Computers & Security* 38 (2013): 97–102, https://doi.org/10.1016/j.cose.2013.04.004.

[5] Bruce Schneier, "Semantic Attacks: The Third Wave of Network Attacks," *Grypto-Gram*, October 15, 2000, https://www.schneier.com/crypto-gram/archives/2000/1015.html#1.

[6] Sara Kraemer, Pascale Carayon, and John Clem, "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities," *Computers & Security* 28, no. 7 (2009): 509–20, https://doi.org/10.1016/j.cose.2009.04.006.

[7] Jonathan McClain et al., "Human Performance Factors in Cyber Security Forensic Analysis," *Procedia Manufacturing*, *6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015,* 3 (2015): 5301–7, https://doi.org/10.1016/j.promfg.2015.07.621.

[8] Martti Lehto, "Cyber Security Competencies: Cyber Security Education and Research in Finnish Universities," in *Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS*, vol. 2015 (C*onference on Cyber Warfare & Security: ECCWS* (Hatfield, UK: Academic Conferences and Publishing, 2015), pp. 179–88.

[9] Harri Ruoslahti et al., "Cyber Skills Gaps – A Systematic Review of the Academic Literature," *Connections: The Quarterly Journal* 20, no. 2 (2022): 33–45, https://doi.org/10.11610/Connections.20.2.04.

[10] R. J. Glavin and N. J Maran, "Integrating Human Factors into the Medical Curriculum," *Medical Education* 37, no. s1 (2003): 59–64, https://doi.org/10.1046/j.1365-2923.37.s1.5.x.

[11] Mica R. Endsley, "Design and Evaluation for Situation Awareness Enhancement," *Proceedings of the Human Factors Society Annual Meeting* 32, no. 2 (October 1, 1988): 97–101, https://doi.org/10.1177/154193128803200221.

[12] G. Fletcher et al., "Rating Non-Technical Skills: Developing a Behavioural Marker System for Use in Anaesthesia," *Cognition, Technology & Work* 6, no. 3 (August 2004), https://doi.org/10.1007/s10111-004-0158-y.

[13] Paul Barford et al., "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situational Awareness: Issues and Research*, ed. Sushil Jajodia et al., vol. 46 (Boston, MA: Springer US, 2010), 3–13, https://doi.org/10.1007/978-1-4419-0140-8_1.

[14] George Tadda et al., "Realizing Situation Awareness within a Cyber Environment," in *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006*, vol. 6242 (*Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006, SPIE)*, 2006, pp. 35–42, https://doi.org/10.1117/12.665763.

[15] Luke Topham et al., "Cyber Security Teaching and Learning Laboratories: A Survey," *Information & Security: An International Journal* 35 (2016): 51–80, https://doi.org/10.11610/isij.3503.

[16] Ibrahim Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," *The Journal of Supercomputing* 74, no. 10 (October 1, 2018): 4986–5002, https://doi.org/10.1007/s11227-018-2337-2.

[17] Lori L. Sussman, "Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers," *Journal of Higher Education Theory & Practice* 21, no. 6 (2021): 19.

[18] Jessica Dawson and Robert Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," *Frontiers in Psychology* 9, no. 744 (2018): 12, https://doi.org/doi: 10.3389/fpsyg.2018.00744.

[19] Sussman, "Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers," (2021).

[20] Robert K. Yin, *Case Study Research: Design and Methods*, 4th ed., vol. 14 (Thousand Oaks, CA: Sage Publications, 2009), https://journals.nipissingu.ca/index.php/cjar/article/view/73.

[21] Pertti Alasuutari, "The Globalization of Qualitative Research," in *Qualitative Research Practice*, ed. Clive Seale et al. (London UK: SAGE Publications Ltd, 2003), 595–608.

[22] Michael Quinn Patton, *Qualitative Research & Evaluation Methods*, 3rd ed. (Thousand Oaks, California: Sage Publications, 2002).

[23] Mathieu Templier and Guy Paré, "A Framework for Guiding and Evaluating Literature Reviews," *Communications of the Association for Information Systems* 37, no. 1 (2015): 112–37.

[24] Philipp Leitner, Mohammad Khalil, and Martin Ebner, "Learning Analytics in Higher Education—A Literature Review," in *Learning Analytics: Fundaments, Applications, and Trends: A View of the Current State of the Art to Enhance e-Learning*, ed. Alejandro Peña-Ayala, vol. 94 (México DF, Mexico: Springer International Publishing AG, 2017), 1–23, https://doi.org/10.1007/978-3-319-52977-6_1.

[25] Hannah Snyder, "Literature Review as a Research Methodology: An Overview and Guidelines," *Journal of Business Research* 104 (November 1, 2019): 333–39, https://doi.org/10.1016/j.jbusres.2019.07.039.

[26] Snyder, "Literature Review as a Research Methodology" (2019).

[27] Paloma de La Vallée et al., "Sector-Specific Training - A Federated Maritime Scenario," in *Multimedia Communications, Services and Security*, ed. Andrzej Dziech, Wim Mees, and Marcin Niemiec (Cham: Springer International Publishing, 2022), 21–35, https://doi.org/10.1007/978-3-031-20215-5_3.

[28] De La Vallée et al.,"Sector-Specific Training - A Federated Maritime Scenario" (2022).

[29] 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): 123–33, https://doi.org/10.11610/isij.4311.

[30] Ilona Frisk, Ilkka Tikanmäki, and Harri Ruoslahti, "Piloting the ECHO E-Skills and Training Toolkit," *Information & Security: An International Journal* 53, no. 2 (2022): 163–75, https://doi.org/10.11610/isij.5311.

[31] Pavel Varbanov, "Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach," *Information & Security: An International Journal* 53, no. 2 (2022): 177–90, https://doi.org/10.11610/isij.5312.

[32] Sten Mäses, Kaie Maennel, and Agnė Brilingaitė, "Trends and Challenges for Balanced Scoring in Cybersecurity Exercises: A Case Study on the Example of Locked Shields," *Frontiers in Education* 7 (September 20, 2022): 1–13, https://doi.org/10.3389/feduc.2022.958405.

About the Authors

Ilkka **Tikanmäki** – see the CV on p. 78 of this volume, https://doi.org/10.11610/isij.5523. https://orcid.org/0000-0001-8950-5221

Harri **Ruoslahti** – see the CV on p. 78 of this volume, https://doi.org/10.11610/isij.5523. https://orcid.org/0000-0001-9726-7956