Information & Security

K. Aaltola & P. Taitto
vol. 43, no. 2 (2019): 123-133
https://doi.org/10.11610/isij.4311

Published since 1998

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

Research Article

Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training

Kirsi Aaltola [a] (✉), *Petteri Taitto* [b]

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

[b] *Savo Consortium for Education, Finland, https://www.sakky.fi/kuntayhtyma/english*

ABSTRACT:

Development of information technology and the globalization require constant investment in people. New and emerging technologies such as autonomous systems, machine learning and AI radically re-contextualize the human dimension of the organization. Strategic changes have revealed new critical vulnerabilities such as social media-based election meddling and disinformation campaigning with impact on the human aspects at state, societal, organizational and individual levels. Education and training raise the level of expertise, skills and competences and ensure better performance in complex cyber situations. Researchers have addressed assumptions, models, concepts and cognitive aspects of human performance in the cyber domain. However, the theories and approaches of human learning in training and exercises are only partly touched. New techniques for enhancing organizational cyber resilience to cyber-attacks are needed and they still lack sound theoretical foundations.

This article aims to advance the discussion suggesting viewpoints on training and exercises in the cyber domain, taking into consideration specifics of skills in cyber security. It provides overview of theories of learning to better support human performance. Our critical interpretation enhances the comprehensive understanding of decision-making, learning theories, and design of cyber security training and exercises. Furthermore, our intention is to constructively promote discussion on current issues about human learning in cyber training and education and thus boost multidisciplinary studies to enhance cyber awareness.

ARTICLE INFO:

RECEIVED: 10 MAY 2019
REVISED: 12 SEP 2019
ONLINE: 18 SEP 2019

KEYWORDS:

cybersecurity, human factors, organizational learning, education and training, exercises

✉ Corresponding Authors: kirsi.hyttinen@laurea.fi; taittopetteri@gmail.com

Introduction

Information technologies are incorporated everywhere in our everyday life and they have shaped our thinking and decision-making processes. Inventing and maintaining technological products and processes will have impact on the world in which people live. Beck claims that reflection is the self-confrontation of unintended consequences of human actions.[1] It has been described, for example, what happens when technology develops faster than societal institutions monitoring technology. Scientific and academic studies have also seen rather challenging evolving threats, digital changes and innovations.[2] The foundations for this positioning employ different scientific disciplines (Information Technology (IT), organizational and management, adult education, cognitive science and psychology of learning). Traditional information security mainly focuses on protection of information sources and the roles of humans in the security processes, when cyber security also sees humans as potential targets of cyber-attacks or participants in a cyberattack.[3] Researchers have considered already a need for multidisciplinary research, with focus on multilevel adult education directions in cyber security education.[4]

Cyberattacks normally use codes to change computer code, data or logic with the aim to result in disruptive consequences that lead to cybercrime.[5] The consequences of cyberattacks vary from identity theft, spoofing, stolen hardware, breach of access, and system infiltration to instant message abuse. Beyond *physical* (e.g. physical outage of power) and *syntactic* (e.g. attack against logic of computer systems) cyberattacks, *semantic* (e.g. targeting the way human perceive or interpret) cyberattacks are seen more serious threats since they target human interface.[6] Therefore, human performance is pertinent issue within cyber security,[7] where human and organizational factors play a significant role in the computer and information security (CIS) vulnerabilities.[8]

Instead of only focusing human in cyber context, considerations to improve capabilities and human competences cyber domain has found the relevance of learning, education and training at the societal level. Improving cyber security competencies boost skills of citizens and professionals in threat preparedness and in managing vulnerabilities and disruptions.[9] Raising interest of researchers as well as practitioners is to analyse human performance already during cyber trainings and exercises that can be considered more proactive learning than experiences during actual cyberattacks. Nevertheless, the considerations mainly screen on education and trainings as information sharing mechanisms and leave out pedagogical models, organizational and learning theories when understanding learning part of expertise and competence development. Approaches like experiential learning or organizational learning theories from concrete experience and reflection towards transformed action broader humans' experiences (to become richer and deeper) [10] could further enrich managing better human performance in cyberattacks.

Purpose and methods

This position paper aims to provide position of current practices and *rethink* considerations of human performance in cyber security trainings and exercises. We focus on consider research and practical *implications* and *construct* beyond current concepts in cyber security trainings and exercises and evaluating human performance.

We analysed collected information from different sources with use of qualitative analysing methods. Qualitative research methods are seen valuable especially when analysing social or cultural phenomena from the participants' point of view.[11] Especially in complex cyber domain the understanding of shared taxonomy and language together with shared meanings are crucial as social constructions. Our analysis is based on reality assumptions of written concepts, and therefore philosophical base is in phenomenology.[12]

Cyber Training and Exercises

Education approaches recognize the transitioning from novice expert through mentoring and participation into community of practice.[13] In 2010 onwards, it was recognized that there would be a rapid shift in education from traditional classrooms to online and virtual environments.[14, 15] The learning spaces extend beyond traditional thinking of a teacher and a classroom. The learning spaces include participation and socialization into a wider community of practice with an involvement as a member, identity formation and experience in the activities of the practice.

The terms *cyber education* and *cyber training* are some of the key terminology. Cyber education is more focused on the acquisition of knowledge and understanding, through which skills are developed. Whereas, training tends to be targeted at the acquisition of skills to a demonstrable level of competence. There is a strong case for engaging in both education and training as part of career development in cyber security and therefore assessing and evaluating competence needs.[16] The term *cyber exercise* is used for a planned event during which an organization simulates a cyber-disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.[17] Cyber exercises train personnel across different organization levels in a simulated learning environment of large-scale cybersecurity incidents that escalate to become cyber crises. The exercises offer opportunities to analyse, train and rehearse advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations. Cyber exercises are based on real-life events, which are further developed to evolving scenarios. The term *cyber exercise methodology* refers to the model of the exercises. Exercises can be both Discussion based (like workshops, tabletop or games) and Operations based (like drills, functional or full-scale exercises).[18]

Humans performing in cyber domain deal with multi-faced disasters and crisis. Simulation exercises are proven beneficial by preparing people to sudden onset hazards. Cyber safety and security exercise platforms provide an opportunity to

analyse human-machine or human-computer interactions or transactions. Analysing tools can measure human performance during the cyber exercises on their cognition or decision-making based on eye tracking or use of mouse or keyboards. Such analyses are normally provided with use of quantitative methods and measures (e.g. number of transitions between software tools).[19] Cyber exercises involve competitive events with teams, including problem solving, decision-making, analysis skills and situational aware- ness. Situational awareness (SA) in cyber security is seen relevant in describing, measuring and predicting human performance. It includes *situation recognition* (e.g. perception of the type of cyberattack, target of the attack, source of the attack), *situation comprehension* (e.g. understanding why and how the situation is caused, and its impacts), and *situation projection* (the expectations of the future, locations and impacts).[20, 21] To more comprehensively consider learning, including knowledge creation, skills, competences and expertise, we could adapt experiential learning and relevance of tacit knowledge in to the discussion of cyber security training and education.

Experiential and organizational learning

Beyond research and studies to be conducted in cyber security, education and training play crucial role in promoting the knowledge we need to develop.[22] We reviewed two key approaches of learning, experiential learning and organizational learning theories, to be introduced more in this chapter. Our viewpoints are elaborated in line with these theoretical considerations.

Experiential learning is broadly defined as "learning from experience" or "learning by doing." Active learning like 'learning by doing' promotes understanding of the experience by involving the participants directly in the experience in relevant context. For instance, experiential education first permits learners with an experience and then facilitates reflection about experiences in order to develop skills, attitudes, or new ways of thinking and competences.[23] The well-known David Kolb's theory of experiential learning has expanded philosophy of experiential education.[24] A foundation of inter-disciplinary and constructivist learning and constructivist approaches are the basis of experiential learning. In cyber domain and cyber security, cognitive approaches are mainstreamed to emphasis the assumptions and building new forms of understanding through activity. This understanding is gained within learning field as well.[25] Experiential Learning Theory (ELT) is a dynamic perspective to learning. It includes dual dialects of action with reflection and experience with abstraction.[26] Active process and understanding create together deeper levels of learning.

Already in 1966 Polanyi concluded that "tacit knowing is such elusive and subjective "awareness" of individual that cannot be articulated in words."[27] Nonaka and Takeuchi continued this dichotomy of knowledge towards organizational learning activities in social interactions.[28] Social interactions among professionals can create knowledge and enhance knowledge environment. According to cyber phenomena, it could be considered that cyber professionals and experts have lot of tacit knowledge they know but they do not tell or explain. More complex cybersecurity field increases within its sectors and their dependencies or

applications and technologies, more complicated it will be for humans and professionals to communicate among people in different level of knowledge.

Our focus on decision-making of cybersecurity professionals is seen dynamic process where analysts interact with task environment with limited information and uncertainty.[29] Taitto et al. argue that the decision-making processes are pivotal in order to prevent further damages and creating necessary protective measures in the cyber related incidents.[30] Exercising these decision-making processes, is often times crucial for the organization's resilience, and require innovative techniques for an increased engagement and more effective results. Helliar and co-authors have explored the risk and decision making of the financial managers, and found that the decision makers have number of systematic biases that that dominates decision-making.[31] Such are over-confidence, representativeness and conservatism, narrow framing, and ambiguity aversion. Over-confidence arises partly from self-attribution bias. This is a tendency on the part of investors to regard successes as arising from their expertise while failures are due to bad luck or the actions of others. This leads to excessive confidence in one's own powers of forecasting.

Decision-making is not always rational, and either the linear decision-making process is not always optimal. Decision making processes have been discussed and studied for example by Leonard and Biberman in several dimensions.[32] They present additional dimensions to classical decision-making theory. Such are for instance tacit knowledge decision models and intuitive decision models. Tacit models encourage managers to draw on their latent cumulative experience in order to improve decision-making. Intuitive decision models draw on the brain's ability to make unconscious correlations that are beyond the conscious mind's capability.

Education, training and exercises should simulate the reality to ensure experiential learning. A good cyber drill encourages decision maker to challenge traditional processes and test intuitive and tacit models. The optimal cyber exercise includes not only exercising on individual level, but also as collective. Those possessing managerial position in the organization should experience the consequences of their decisions in a safe learning environment providing opportunity for action and reflection. To provide opportunity to wider and deeper learning, organizational learning theories could be tested and adapted among professionals working in cyber domain.

Consequently, when considering learning in education and training, we automatically face training planning aspects. Outcome needs in curriculum planning helps directing the learning towards common goal and measuring it. Back in the days, already Greek philosophies, like Aristotele and Plato, final causality suggested that "purpose can incite action."[33, 34] The learning outcome captures the preceding training needs analysis and should contain a metric to assess learning. Therefore, the outcome needs to be SMART (specific, measurable, achievable, realistic and time-based) and thus the outcomes are defined in a constructive alignment process, where learning outcomes are defined using measurable terminology.

Training and exercise design

The diversity of threats and their reach compel states to build a strong cyber security strategy including education and training aspects. Training design should therefore acknowledge that the evolving nature of cyber space as itself creates new requirements. In every training and exercise design, setting the learning objectives is in the nucleus of the process. Simulation based exercises are means to transfer outcomes defined in the curriculum in to the practice. In some cases the online education is following a trend of using teaching technology, or teaching machines, dating back to the 1950s.[35] Moreover, the educational institutes still lack proven design approaches for complex learning that involves integration of skills, knowledge, attitudes and adapting them to real life context.[36] Cyber training and exercises will raise even more complex design challenges.

To enhance and raise the effectiveness of learning in cyber training, there are research findings around narrative-based and tool-based trainings, personalities in team performance and cognitive aptitude.[37] Like in any field, also within cyber domain, people should know how to use the products, services or systems.[38] Designing intelligent training and exercise systems like cyber ranges require simulation of human cognitive processes and for example decision-making processes. That is why methods for designing are important. Specialists of human technology interaction will need to meet with this challenge on designing technologies with intelligent capacities.[39] Purpose of human-centred design is to create technological solutions easy to use and commit community of practices can support design in cyber training.

The innovative and cost-effective technological solutions like cyber ranges in cyber education architectures can illustrate the strength of experiential learning of skills and competencies through simulated scenarios, role-playing, problem-solving and visual observations in cyber training contexts. Simulation based exercises connect learning, simulation and gaming aspects in an innovative way imitating reality by using virtual environments or virtual programs in a way where computer-assisted games are integral part of learning environment.

Conclusions

Responding to crisis, preparedness and building resilience requires multidisciplinary approaches. Cyber domain is one of the disciplines, not only as one among the others, but crosscutting issue in every function in every organization and society. As human behaviour and decision-making in particular, play a crucial role in the cyber security, the training and exercising should simulate this reality as well as possible.

First, we found that considering cyber education and training in respect to experiential learning principles deepens the level of learning. Developing human skills and competence in cyber domain should be seen as a constructive process, where learner's previously adapted competences are recognized and utilized. Learning process begins always by screening what competences participants have and these competences can be utilized to enhance others' learning process. Experiential learning approach can create framework and theoretical basis for holistic

approach training and exercise system. Knowledge, competences and expertise needed in complex multifaceted crisis environment is therefore mutually built and constructed across organization members. To infuse learning and ensure competitiveness for organizations utilizing explicit and tacit knowledge together later on become powerful engine.[40, 41, 42] The approaches of learning could be further utilized and conceptualised in cyber security training, education and exercises to better prepare human performance especially on skills like decision-making.

The traditional assumption of the optimality of rational decision-making may be improved by including other dimensions of decision-making. It is posited that organizations that encourage and support multi-dimensional decision making, which utilizes the rational, intuitional, emotional and spiritual aspects of the whole person, develop better management–employee relations, more creative problem solving, and better market place performance.[43] Leonard and Biberman argue against the classical decision theories that are based on the assumption that decision makers are rational, and make reasoned choices based on their analysis of the risks and rewards of the situation.[44] Instead of making decision consciously there are number of bias in every decision making process, and therefore exercises can be seen as important factor shaping the models of decision-making. It is important to improve such practices that best improve decision-making, taking into the consideration the characteristics of the decision maker. Knowing yourself, the self-reflection is the key for improvement of any decision maker. Intuitive and tacit decision-making theories can be aligned through training and exercising, thus making the models more systematic.

Consequently, we suggest research community in close cooperation with practitioners and user communities to study more human performance and human aspects in cyber training from learning perspective with transfer of intelligent cognitive behaviour. It could be suggested to include more design perspectives of human-technology interaction also to cyber training and exercises to improve human performance in actual cases.

Acknowledgement

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943. European Commission funded cyber pilot projects like 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.

References

1 Ulrich Beck, *Risk Society. Towards a New Modernisation* (London: SAGE, 1992); and Ulrich Beck, "Cosmopolitical Realism: On the Distinction Between Cosmopolitanism in Philosophy and the Social Sciences," *Global Networks* 4, no. 2 (2004): 131-156.

[2] Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, Gian-Luigi Ruzzante, Nineta Polemi, and Malgorzata Figwer, "European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy," EUR 29332 EN (Luxembourg: Publications Office of the European Union, 2018), p. 5, https://doi.org/10.2760/622400, JRC111441.

[3] 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.

[4] Eleni Berki, Juri Valtanen, Sunil Chaudhary, and Linfeng Li, "The Need for Multi-Disciplinary Approaches and Multi-Level Knowledge for Cybersecurity Professionals," in *Multi-disciplinary Perspectives on Human Capital and Information Technology Professionals* (IGI Global, 2018), p. 72, https://doi.org/10.4018/978-1-5225-5297-0.ch005.

[5] Berki et al.,"The Need for Multi-Disciplinary Approaches and Multi-Level Knowledge for Cybersecurity Professionals."

[6] Bruce Schneier, "Semantic Attacks: The Third Wave of Network Attacks," *Crypto-Gram*, October 15, 2000, accessed September 2, 2019, https://www.schneier.com/crypto-gram/archives/2000/1015.html#1.

[7] Jonathan McClain, Austin Silva, Glory Emmanuel, Benjamin Anderson, Kevin Nauer, Robert Abbott, and Chris Forsythe, "Human Performance Factors in Cyber Security Forensic Analysis," *Procedia Manufacturing* 3 (2015): 5301-5307.

[8] Sara Kraemer, Pascale Carayon, and John Clem, "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities," *Computers and Security* 28 (2009): 509-520, https://doi.org/10.1016/j.cose.2009.04.006.

[9] Martti Lehto, "Cyber Security Competencies: Cyber Security Education and Research in Finnish Universities," *Proceedings of the 14th European Conference on Cyber Warfare & Security*, Hatfield, UK, University of Hertfordshire, July 2-3, 2015, pp. 179-188, quote on p. 179, http://ti- nyurl.com/ECCWS2015.

[10] Alice Y. Kolb and David A. Kolb, "Experiential Learning Theory: A Dynamic, Holistic Approach to Management Learning, Education and Development," in *The SAGE Handbook of Management Learning, Education and Development*, edited by Armstrong and Fukami (SAGE Publications, 2009), p. 13.

[11] Bonnie Kaplan and Joseph Alex Maxwell, "Qualitative Research Methods for Evaluating Computer Information Systems," *in Evaluating Health Care Information Systems: Methods and Applications*, edited by J.G. Anderson, C.E. Aydin and S.J. Jay (Thousand Oaks, CA: Sage, 1994), 45-68.

[12] See, for example, R. Boland, "Phenomenology: A Preferred Approach to Research in Information Systems in Research Methods," in *Information Systems*, edited by E. Mumford, R.A. Hirschheim, G. Fitzgerald, and T. WoodHarper (Amsterdam: North Holland, 1985), 193-201.

[13] Alice Y. Kolb and David A. Kolb, "Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education," *Academy of Management Learning & Education* 4, no. 2 (2005): 193–212, quote on pp. 199-200.

[14] Elaine Allen and Jeff Seaman, *Class differences: Online education in the United States, 2010* (Babson Park, MA: Babson Survey Research Group, 2010).

[15] Robb Lindgren and Mina Johnson-Glenberg, "Emboldened by Embodiment: Six Precepts for Research on Embodied Learning and Mixed Reality," *Educational Researcher* 42 (2013): 445–452.

[16] K. Blaine Lawlor and Martin J. Hornyak, "Smart Goals: How the Application of Smart Goals Can Contribute to Achievement of Student Learning Outcomes," *Developments in Business Simulation and Experiential Learning* 39 (2012).

[17] See the definition for "cyber exercise" in Joaquin Jay Gonzalez III and Roger L. Kemp, eds., *Cybersecurity: Current Writings on Threats and Protection* (Jefferson, NC: McFarland, 2019), p. 239.

[18] Spanish National Cybersecurity Institute, "Cyber Exercises Taxonomy," 2015.

[19] McClain, et al.,"Human Performance Factors in Cyber Security Forensic Analysis."

[20] George Tadda, John J. Salerno, Douglas Boulware, Michael Hinman, and Samuel Gorton, "Realizing Situation Awareness within a Cyber Environment," in *Proceedings of Defense and Security Symposium*, Orlando (Kissimmee), Florida, United States, vol. 6242 (2006), https://doi.org/10.1117/12.665763.

[21] Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, *Cyber Situational Awareness* (New York: Springer, 2010).

[22] UNESCO, "Rethinking Education – Towards Common Goal?" p. 66.

[23] Linda H. Lewis and Sarol J. Williams, "Experiential Learning: Past and Present," *New Directions for Adult and Continuing Education* 62 (1994): 5-16.

[24] Farooq Mughal and Aneesa Zafar, "Experiential Learning from a Constructivist Perspective: Reconceptualizing the Kolbian Cycle," *International Journal of Learning & Development* 1, no. 2 (2011): 27-37.

[25] Sara de Freitas and Jill Jameson, *The E-Learning Reader* (London and New York, Continuum Books, 2012).

[26] Kolb and Kolb, "Experiential Learning Theory: A Dynamic, Holistic Approach to Management Learning, Education and Development," p. 43.

[27] Michael Polanyi, *The Tacit Dimension* (New York: Anchor Day Books, 1966).

[28] Ikujirō Nonaka and Hirotaka Takeuchi, *The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation* (New York, NY: Oxford University Press, 1995).

[29] Ian A. Cooker, Alexander Scott, Kasia Sliwinska, Novia Wong, Soham V. Shah, Jihun Liu, and David Schuster, "Towards Robust Models of Cyber Situation Awareness," in *Advances in Human Factors in Cybersecurity,* edited by Tareq Z. Ahram and Denise Nicholson, Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Orlando, Florida, USA, in *Advances in Intelligent Systems and Computing*, vol. 782 (Cham: Springer, 2018), 127-137.

[30] Petteri Taitto, Julia Nevmerzhiskaya, and Csaba Virag, "Using Holistic Approach to Developing Cybersecurity Simulation Environments," *eLearning & Software for Education* 4 (2018): 77-84, https://doi.org/10.12753/2066-026X-18-226.

[31] Christine Helliar, Alasdair Lonie, David Power, and Donald Sinclair, *Attitudes of UK Managers to Risk and Uncertainty* (Edinburgh: The Institute of Chartered Accountants of Scotland, 2001).

[32] Barbara Leonard and Jerry Biberman, "Utilizing Multi-dimensionality in the Workplace: A Meta-study," *Managerial Finance* 33, no. 12 (2007): pp. 935-946.

[33] Claude S. George, *The History of Management Thought* (Englewood Cliffs, NJ, Prentice-Hall, Inc. 1972).

[34] K. Blaine Lawlor and Martin J. Hornyak, "Smart Goals: How the Application of Smart Goals Can Contribute to Achievement of Student Learning Outcomes," *Developments in Business Simulation and Experiential Learning* 39 (2012): 259-267.

[35] Nuri Kara and Nese Sevim, "Adaptive Learning Systems: Beyond Teaching Machines," *Contemporary Educational Technology* 4, no. 2 (2013): 108-120.

[36] Jeroen J. G. van Merrienboer and Paul Kirschner, *Ten Steps to Complex Learning: A Systematic Approach to Four-Component Instructional Design*, Third Edition (New York, Routledge, 2018), p. 2.

[37] See for example Susan Stevens-Adams, Armida Carbajal, Austin Silva, Kevin Nauer, Benjamin Anderson, Theodore Reed, and Chris Forsythe, "Enhanced Training for Cyber Situational Awareness," in *Foundations of Augmented Cognition*, edited by Dylan D. Schmorrow and Cali M. Fidopiastis, *Lecture Notes in Computer Science*, vol. 8027 (Berlin, Heidelberg: Springer, 2013), 90-99, https://doi.org/10.1007/978-3-642-39454-6_10.

[38] Jaana Leikas and Pertti Saariluoma, "'Worth' and Mental Contents in Designing for Ageing Citizens' Form of Life," *Gerontechnology* 7, no. 3 (2008): 305-318.

[39] Pertti Saariluoma, Antero Karvonen, Mikael Wahlstrom,Kai Happonen, Ronny Puustinen, and Tuomo Kujala, "Challenge of Tacit Knowledge in Acquiring Information in Cognitive Mimetics," in *Proceedings of the 2nd International Conference on Intelligent Human Systems Integration (IHSI 2019): Integrating People and Intelligent Systems*, February 7-10, 2019, San Diego, California, USA, edited by Waldemar Karwowski and Tareq Ahram, 228-233.

[40] Meng Li and Fei Gao, "Why Nonaka Highlights Tacit Knowledge: A Critical Review," *Journal of Knowledge Management* 7, no. 4 (2003): 6-14, https://doi.org/10.1108/13673270310492903.

[41] Polanyi, *The Tacit Dimension*.

[42] Nonaka and Takeuchi, *The Knowledge Creating Company*.

[43] Barbara Leonard, *Multidimensional Decision Making*, Ebook (Bradford: Emerald Publishing, 2007).

[44] Leonard and Biberman, "Utilizing Multi-dimensionality in the Workplace: A Meta-study."

About the Authors

Kirsi **Aaltola** (MA, PhD Candidate) is currently acting as a Senior Manager for Research at Laurea UAS. She has a strong experience with coordination of wide networks through various international projects (funded by "Horizon 2020," the Seventh Framework Programme, by EC general directorates or regionally funded) and design and implementation of different training and higher education training programs in the field of security. She is a PhD candidate in the University of Jyväskylä, finalising her doctoral thesis related to the human-centred approach in the design of technologies and analysing human-technology interaction. Her research interests include information management technologies and their design with theoretical HCI understanding in the safety and security fields. In 2009-2014 she has run international crisis management courses such as EU Concept Core Courses, Pre-Deployment Trainings (also under ENTRi framework), Hostile Environment Awareness Training (HEAT) and UN/NATO/IHP led humanitarian/civil protection large scale exercises.

Petteri **Taitto** (MA, General Staff Officer) is currently holding the position of Head of Development at the Savo Consortium for Education in Kuopio, Finland. Petteri has previously held positions of Principal Scientist in Laurea UAS and in the European External Action Service as an operations planner and training coordinator for EU CSDP Mission related training programmes at the European Security and Defence College. He has also developed and implemented training programmes for civilian crisis management when working as CMC Finland's Head of Training. His other earlier appointments include Principal Lecturer and education programme leader at the Emergency Services College, and various assignments in Finnish Defence Forces, including teacher at the National Defence University. His research interests have focused on EU integrated approach for security and educational implications in professional crisis management training.