5th International Conference on Higher Education Advances (HEAd'19)
Universitat Politècnica de València, València, 2019
DOI: http://dx.doi.org/10.4995/HEAd19.2019.9305

The Joint Effort Workshop as a tool for Knowledge Management and competence development

Markus Bresinsky, Florian Reusner, Miriam Pöhner
Faculty of General Studies and Microsystems Engineering, Ostbayerische Technische Hochschule Regensburg (OTH), Germany.

Abstract

Cybersecurity is a complex global phenomenon where the risks for individuals, organisation and the society are rising day by day. These risks need to be identified and analysed in order to spread prevention and elaborate countermeasures. In this paper, we describe the Joint Effort Workshop 2019 as an approach to raise awareness to these threats and to generate and share knowledge about Cybersecurity and Critical Infrastructure between students and field experts.

We believe that mechanisms for systematic response to attacks need not only the developed technical requirements, but also a deep understanding of the human behaviour, knowledge and resilience to response to risks. This approach towards knowledge and practical training can be experienced through the collaborative environment of the Joint Effort Workshop.

Keywords: *Virtual Collaboration; Knowledge Management; Organizational Learning; Cybersecurity; Critical Infrastructure; Collaborative Learning.*

1. Introduction

A globalised and internationally connected world entails consequences on individual and organisational level, where especially in the field of Critical Infrastructures and Cybersecurity the risk and impact is most visible. Since events like the Cyberattack on Estonia in 2007, the ongoing massive attacks through Fake News on multiple levels of any democracy, hacking sensible data and passwords or the chain reaction of interconnected supply facilities in the water, energy or communication sector, the public attention towards these topics has increased. The demands of digital technologies and steadily interconnection is redefining the way how to deal with collaboration and communication. Here, interdisciplinary and systematic while simultaneously flexible approaches in education and application are needed. Higher education institutions like the OTH Regensburg are facilitators and enablers of creating ways to prepare and educate young professionals for the upcoming challenges. Research as well as experienced experts propose effort on hands-on learning and experiencing to prepare young professionals for challenges and crisis management through education (Senge, 1990, Carell, 2004, BBK, 2011, UN OCHA, 2018). Furthermore, there are different ways to tackle these challenges and to implement digital literacy, raise awareness on current fields of concern and to develop a set of skills are investigated and outlined (EC, 2011, HFD, 2016, NMC, 2017, Kolb, 1984). One practical approach, where students, managers and experts can exchange and interact to generate knowledge and develop competences is the later presented Joint Effort Workshop concept.

The paper presents how to face the challenges of the technological and digital change with a hands-on approach in higher education in collaboration with experts and organisations through the Joint Effort Workshop. We first briefly examine the work environment. Later we outline the concept of Organisational Learning (OL) and Knowledge Management (KM), before we introduce the concept of the Joint Effort Workshop, as a tool for competence development, Knowledge Management and as an innovative environment. The paper concludes by describing the advantages of the learning concept for organisations and individuals likewise.

2. Work Environment and Characteristics

As technology and digitalisation is shifting the workplace towards a virtual environment, using Information and Communication Technology (ICT) and digital tools and loosen structures like hierarchy, organisations and centralisation, it can have positive consequences like increased productivity, saving resources and opening global opportunities. Anyhow, negative impact and even threats are arising within this change of interconnectivity and behaviour in the virtual environment. The high risk of all interconnected infrastructure consists of being vulnerable to cyberattacks. Thus, globalisation and virtual organisation need

adapted global structures and processes, as humans as users are in need of a comprehensive awareness, understanding and set of skills to be able to meet these demands.

2.1. Virtual Collaboration

Since the implementation of technological developments and digital advances in nearly all sectors, the virtual collaboration and communication is omnipresent. It means an independent and dedicated working process of a group of individuals who pursue a common goal, collaborating and communicating to overcome spatial, temporal and organisational obstacles by electronic means (Lipnak & Stamps, 1998, Wainfan & Davis, 2004). This entails new structures like asynchronous group work in a virtual space and shifted leadership and management focus. In addition, this leads to face ways of shared responsibilities, cultural and language challenges, and implicated risks in knowledge management and also cybersecurity.

Data and information are always and everywhere accessible and retrievable which has impact on the flexibility of the work environment and processes and the vulnerability of the system itself. Through the close connection of technological means, cooperation, collaboration and knowledge exchange are getting easier, as we can see with the Internet of Things (IoT) or Smart City approaches. The positive opportunities of technological developments are accompanied by rising computer-related crimes, exploiting system vulnerabilities aiming at illegal activities to make profit or causing harm. Cybersecurity is one part of the Critical Infrastructures of a nation or an organisation, which is subject to multiple threats. Therefore, collaborative effort to develop strategies and concepts have to be started to manage activities like raising awareness of the threats itself and to start defending public and individual safety against vulnerabilities or attacks (Solms & Niekerk, 2013). To keep up with this complexity of threats and to learn from experience, we must focus on the early phases and the scenario preparation before attacks occur, to create a basis and common ground for detection, prevention and crisis management. Collaboration and information sharing about vulnerabilities, threats and processes can improve the overall security, but the actual implementation of a common approach is interfering with an organisational or individual agenda. The complete process takes time, resources and trust. To overcome these difficulties standards and processes should be developed. In the following part we explain Organisational Learning (OL) and the Knowledge Management (KM) as a possibility to serve as the first step towards an actionable approach.

2.2. Organisational Learning and Knowledge Management

Every organisation and company is using collaboration networks or tools, like Slack, Trello, Adobe Connect, Sharepoint or cloud solutions, to provide a digital workspace to communicate, store and exchange information, share ideas and manage projects. The knowledge is the heart and soul of every organisation, even more since it is often recognised

as the 4th production factor (alongside land, labour and capital). Therefore, organisations face knowledge and information at large, as the crucial factor for their ventures. Knowledge has to be organised and planned to serve for individual and organisational success. At latest since Argyris and Schön (1978) introduced the concept of "Organisational Learning", and Senge (1990) the "Learning Organisation", a common understanding of the need of an adapted behaviour towards a successful future is ongoing.

Learning is known as the dynamic development of individuals while detecting and correcting errors, and one could argue that the commutation of the individual knowledge is the first step of organisational learning, where the generated knowledge can be stored and exchanged. (Schein, 1992). While OL is focusing on the processes, KM attempts to acquire, create, process and utilise the generated knowledge (Easterby-Smith & Lyles, 2003). The goal is to continuously improve practices and behaviours in learning cycles.

The technological developments and change lead to an adaption of education approaches to embed the real-life education to experience and problem-based learning collaborating on platforms and innovative environments interlinking with experts and in-field organisations. These approaches will have a positive impact on lifelong learning, skills development and networking to tackle current and future challenges through the participatory hands-on experience of the participants in an activating and empowering real-life setting where knowledge is applied and skills developed.

To be able to generate knowledge, it would be necessary to implement collaborative efforts with learning and experiencing. The OL can serve as a tool to improve effectiveness, enable change of perspective and understand the complexity of challenges as well as provide the environment of information and knowledge exchange to preparation of risks. One possibility to provide such an environment is through the presented Joint Effort Workshop.

3. The Joint Effort Workshop

The Joint Effort Workshop 2019 is part of a project series on multinational, trans-organizational and intercultural collaboration. The purpose is to tackle current issues and develop solutions through virtual cooperation allowing scholars from all over Europe to take part. A combination of input from subject matter experts and research conducted by the participating students support this task.

The workshop in 2019 addressed the topic of Critical Infrastructures and Cybersecurity. While the protection of Critical Infrastructures and their risk of cyberattacks has been of current discussion throughout the years, knowledge on this up-to-date topic is still very low among scholars. Thus, the workshop aims at creating awareness for students by providing

expertise on Critical Infrastructures and Cybersecurity including definitions, national and European legislation, incidents and European cooperation.

Throughout the workshop, students will conduct research, present their results, and actively participate in discussions with experts of an international context through virtual collaboration. The workshop supports the participants' problem solving, team working and communication skills.

3.1 History and Concept

The .dot platform serves as a mean for transferring knowledge and further education, and advanced training in the field of virtual collaboration. For this purpose, the .dot platform is the basis for most diverse qualities of sustainable acquisition and transfer of knowledge deriving from multinational and multicultural collaboration. Since 2012, different project groups of students of the study program "International Relations and Management" at the OTH Regensburg under supervision of Prof. Dr. Markus Bresinsky fill the platform with their distinct projects, namely the Joint Effort Series, the GLOBE Exercise and various Summer Schools.

The focus of this paper is the Joint Effort Workshop where the following projects have been implemented over the last years:

- "Shared Situational Awareness Workshop" (2013/14)
- "Joint Effort Ivakale" - training and collaboration in a fictive scenario on development cooperation with real partners in Ivakale/Kenia (2014/15)
- "Joint Effort Virtual Multinational Exercise" - Improving the long-term prospects for potential migrants from Africa in their home countries through development cooperation (2015/16)
- "Joint Effort big.dota Workshop" - Bringing together Data Analysts and Social Scientists (2016/17) and the
- "Joint Effort Workshop 2019" - Virtual Collaboration on Cybersecurity (8.-9. February 2019)

During the Joint Effort Workshop 2019, students are going to work at their home university and virtually with students from universities across Europe on the challenges and opportunities of Cybersecurity while training virtual competencies. Special focus will be put on the protection of Critical Infrastructure.

The two-day workshop will start with a general expert input on Cybersecurity and Critical Infrastructures. Following that, students will conduct research themselves on the status quo in their home countries (U^1), answering questions such as: What regulations and strategies concerning Cybersecurity and Critical Infrastructure already exist in your country?

Once participants have an understanding of the situation in their respective country, they will tackle the issue from a more practical approach. They will gather information about a cyberattack that happened in their home country and with their newly acquired insights, they will brief students from the other European universities and exchange information in a virtual conference. The day will end with a expert session on how to organize the knowledge gained on the first day.

On the second day, students will have the chance to hear about hacking. In the next step, they will discuss possible challenges and opportunities for international cooperation. Experienced professionals will support the discussion by joining in international virtual groups (U^1, U^2, U^3). Additionally, input is provided by an expert on international cooperation on Cybersecurity and Critical Infrastructures.

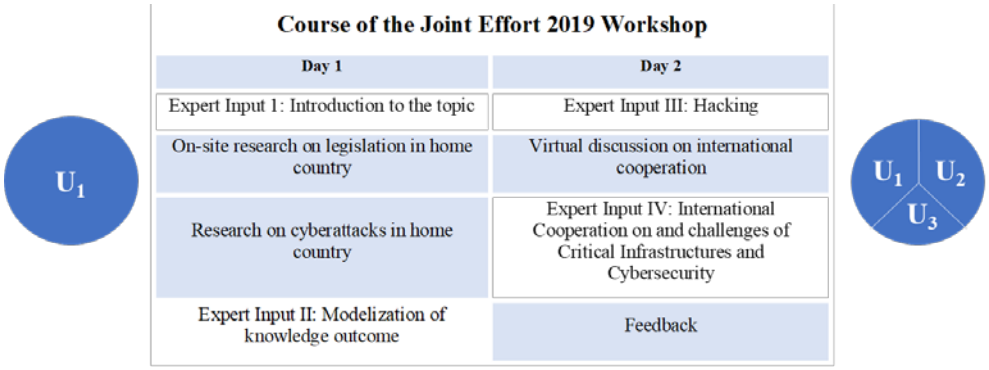

Figure 1 Course of the Joint Effort Workshop 2019. Source: Own figure (2019).

The Workshop concludes with a joint feedback session, where all participants come together to discuss the generated results and give their view about the content and proecedure of the workshop.

3.2 Learning Objectives and Intended Outcomes

Recognising the importance of sharing information about crises, incidents and information and to raise awareness of the context itself, the workshop aims to create an environment where cross-sectional participants can exchange information and ideas and to get introduced to this important topic of Cybersecurity and Critical Infrastructures.

Placing the workshop setting into academic context, a safe and secure environment to train, experience and create ideas with simultaneously connecting students and experts for future development and innovation in the field is possible. The main focus is to actively engage

participants, create a network and enable learning and ideation with knowledge creation and exchange. For an overview, the main objectives are visualized in the following figure:

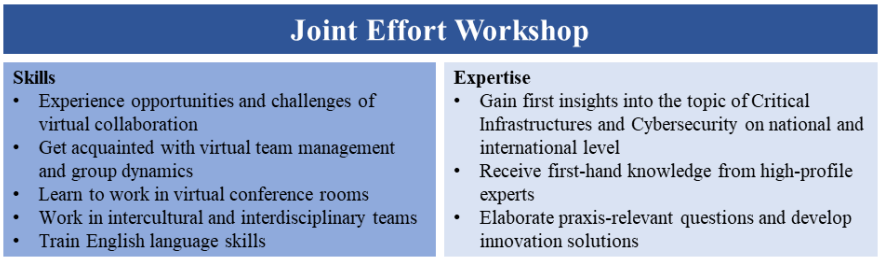

Figure 2 Learning Objectives Joint Effort Workshop 2019. Source: Own figure (2019).

4. Conclusion

In this paper, we have described the possibilities of the Joint Effort Workshop to enhance learning and development aside of raising awareness in the field of Cybersecurity and Critical Infrastructures. The collaborative environment, connecting students and experts through interaction, discussion and feedback sessions, provides the advantage to create and later exchange knowledge which can be used in real-life. Where students learn new knowledge and ideate or innovate in the topics, experts and society benefit from the innovative character.

Through experience and feedback from previous workshops, we have determined that although collaboration and knowledge exchange between students and experts would be beneficial to everyone involved, several barriers to efficient collaboration exist, such as obstacles in the virtual collaboration and communication, information and data management exchange with privacy. Whereas, the overall feedback is positive and experts highlight the innovation and creation of new ideas. Moreover, students are keen to experience real-life involvement in a virtual environment on a challenging important topic. We argue that there is a need to interweave the threats of complex security challenges and human behaviour in order to develop awareness and solutions for current and future risks, especially in the rising fields of Critical Infrastructures and Cybersecurity. The workshop enables participants to test and improve both their theoretical and practical knowledge sharing impressions, processes and methodologies. This last aspect, in particular, facilitates the mutual sharing of different levels of knowledge and expertise in order to find new approaches and possible solutions to the problems analysed. In addition, there is the chance to develop durable networks that will help students and field experts to connect and share innovative ideas. These last aspects totally fit with our vision of Joint Effort. Our workshop aims to develop awareness on the concept of resilience, Cybersecurity and Critical Infrastructure in an innovative environment where students and experts debate and develop new ideas.

References

Adams Becker, S., Cummins M., Davis A., Freeman A., Hall Giesinger, C., and

Ananthanarayanan, V. (NMC) (2017). NMC Horizon Report: 2017 Higher Education Edition. Austin, Texas: The New Media Consortium.

Argyris, C., and Schön, D. (1978). Organisational Learning - A Theory of Action Perspective, Reading.

Carell, L. F. (2004). Leadership in Krisen. Ein Handbuch für die Praxis, Bern

Easterby-Smith, M., and M. Lyles (2003). The Blackwell handbook of organizational learning and knowledge management. Oxford. Blackwell.

European Commission Bureau of European Policy Advisors (EC) (2011). Empowering people, driving change. Social innovation in the European Union. https://doi.org/10.2796/13155

Federal Office of Civil Protection and Disaster Assistance (BBK) (2011). Guideline for

Strategic Crisis Management Exercises. Bonn

Hochschulforum Digitalisierung (HFD) (2016). The Digital Turn – Hochschulbildung im digitalen Zeitalter. Arbeitspapier Nr. 27. Berlin: Hochschulforum Digitalisierung.

Kolb D. (1984). Experiential Learning: Experience as the Source of Learning and Development. Prentice-Hall, Englewood Cliffs

Lipnack, J., Stamps, J. (1998). Virtuelle Teams: Projekte ohne Grenzen; Teambildung, virtuelle Orte, intelligentes Arbeiten, Vertrauen in Teams. Wien.

Schein, E. H. (1992). Organizational Culture and Leadership. John Wiley & Sons

Senge, P. (1990). The fifth discipline: the art and practice of the learning organization. New York: Doubleday.

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) (2018).

United Nations Humanitarian Civil-military Coordination (UN-CMCoord) Field Handbook. Version 2.0. Geneva, Switzerland.

von Solms, R., van Niekerk, J.(2013). From information security to cyber security.

Computers & Security 38, 97 – 102 (2013), cybercrime in the Digital Economy

Wainfan, L., and Davis, P. (2004). Challenges in virtual Collaboration. RAND. National

Defense Research Institute. 2004, Santa Monica, USA http://www.rand.org/content/dam/rand/pubs/monographs/2004/RAND_MG273.pdf