Information & Security

Published since 1998

Sabi I. Sabev
vol. 44 (2020): 76-92
https://doi.org/10.11610/isij.4407

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

Research Article

Integrated Approach to Cyber Defence: Human in the Loop Technical Evaluation Report

Sabi I. Sabev

15 Buzemska str., bl.2, entr. A, 1618 Sofia, Bulgaria

ABSTRACT:

This report provides an overview and critical discussion of the HFM-288 Research Workshop. The workshop was designed to address the critical aspects of the integrated approach to cyber defence with focus on the role of human factors to cyber resilience and to generate solutions to greatly improve the role of people in fighting the cyber threats. Four keynote speakers and 24 presentations provided a variety of perspectives on the issues. Discussions revealed that there is significant shared understanding amongst the researchers and experts on the increasing role and responsibilities of humans in building a robust and resilient cyber security and defence. This report concludes with recommendations on areas where current efforts need to be consolidated, and areas where continued efforts are required.

ARTICLE INFO:

RECEIVED: 09 Mar 2019
REVISED: 10 May 2019
ONLINE: 22 JUNE 2019

KEYWORDS:

cyber defence, cybersecurity, human factors, research, operations, education & training

Creative Commons BY-NC-SA 4.0

Introduction

The HFM-288 Research Workshop (RWS), held 16-18 April, 2018, in Sofia Bulgaria, was organized by NATO STO HFM Research Task Group "Human system integration approach to cyber security" (NATO STO HFM – 259 RTG). During the Research Workshop thirty-seven authors from nine NATO and Partnership for Peace nations submitted 28 presentations in the three days of the workshop.

E-mail: sabsismal@gmail.com

Four keynote presentations in two sessions were delivered the first day, followed by seven topic sessions in the next two days of the workshop. This Technical Evaluation Report summarizes the core ideas and results presented during this workshop. The report also provides an overview of the presentations and discussions in all sessions of the workshop and concludes with summaries of messages and recommendations. All sessions of the Workshop were unclassified.

The concept for this research event suggested nine topics to be covered during the HFM – 288 RWS:

- Identification and mitigation of potential cyber security vulnerabilities at organizational and individual levels;
- Recruitment, selection, training and maintenance of the cyber force;
- Cyber security awareness training, monitoring and assessment;
- Abilities and capabilities that are essential for organizational resilience to cyber-attacks;
- Ethics of using cyber systems to influence operator and user behaviour (ROE);
- Improving human-machine interfaces (reducing complexity of security systems; trust and openness in networked information and network-based interactions, etc.);
- Application of human performance and cognitive modelling for identification of potential cyber security vulnerabilities in the human aspects of cyber systems;
- The role of safety culture in relation to cyber defence;
- Best practices and shortfalls for cyber defence policies implementation, as well as Education and Training (E&T) programs to improve the security of human behaviour.

The general concept for an Integrated Approach to Cyber Defence, centred on the human behaviour in the cyber domain, has been recognized as a missing block in building and sustaining robust cyber security systems in the rapidly growing and dynamic cyber space.

Recognizing the value of this research domain, HFM-288 RWS was organized to achieve the following goals:

- To promote cyber security system thinking including the Human Factors in defence domain;
- To explore and address the range of Human Factors topics/ issues relevant to cyber security; and
- To summarize conclusions and recommendations for how Human Factors can enhance cyber defence in national and allied formats.

The three-day workshop was designed to identify various aspects of the key role and responsibilities of the human factor in building resilient cyber security

and cyber defence systems. Bringing together civilian policy makers, military leaders at strategic and operational level, cyber security experts, academia, IT industry and non-governmental organizations, the workshop organizers created a collaborative environment for intensive discussion and sharing of ideas on the enhanced role of the human factor in fighting cybercrimes and cyberattacks. A challenge to all participants was to provide a solid research basis for developing concepts and approaches to keep humans in the loop in building and sustaining a resilient cyber defence in military and non-military organizations. The final product of the workshop is to be published in the international journal "Information and Security," with a subsequent book publication of selected papers.

Research Background

The research on "Human Systems Integration Approach to Cyber Security" was launched in July 2015 by the HFM – 259 RTG as recognition that the human factor is the cyber systems weakest link, which needs to be transformed into a powerful resource to detect and mitigate developing cyber threats. The 2018 HFM-288 RWS is a direct follow up of the international conference, held 28-29 September 2015 in Sofia Bulgaria. The conference was co-organized by Defence Advanced Research Institute (DARI) at G.S. Rakovski National Defence College - Bulgaria, AFSEA Sofia Chapter and the HFM – 259 RTG[1]. A broad range of topics, linked to the human factors in cyber space and cyber security were discussed at that conference. Seven of its participants took part in the HFM – 288 RWS. The overall theme of this workshop "Integrated Approach to Cyber Defence: Human in the Loop" is meant to deepen the research with focus on the key role of the human factor in building resilient cyber defence systems. Some research topics of this workshop have been a subject to other scientific events, for instance the Symposium on "Cyber Defence Situation Awareness," held from 3-4 October 2016 in Sofia Bulgaria (STO-MP-IST-148). The workshop was also based on the available studies on various issues associated with the cyber threats and cyber security.

Research workshop description and discussion

Opening Address

The workshop opened with an address by Deputy Minister of Defence LtGen (ret.) Atanas Zapryanov who welcomed all participants of the workshop and stressed the importance of this NATO STO research event hosted by Bulgaria. His believes were that the Bulgarian scientists and researchers will be proactive and take leadership in projects where Bulgaria will be able to provide expertise, as is the case of HFM Panel RTG "Human system integration approach to cyber security." He assured of the continuous support by the Bulgarian Ministry of Defence for research activities on promoting cyber security system thinking with focus on the Human Factor, with understanding that human factors are critical in the effective responses to developing complex cyber threats. At the end he underlined the adoption of the Bulgarian Cyber Security Strategy in

2016, which implementation will be strengthened by the new Cyber Security Law, to be promulgated by the Bulgarian National Assembly in 2018.

The welcoming remarks from the Bulgarian host – Capt (BGR-N) Prof. D.Sc. Yantsislav Yanakiev highlighted the NATO STO HFM – 288 RWS goals and the broad international and national participation in the workshop, both scientists and researchers, and attendants.

Presentations

First Keynote Session

The first session included two keynote presentations under the general theme of the workshop. The initial presentation was the keynote address by Mr Alan R. Shaffer, Director of Collaboration Support Office at NATO STO, who stressed the changing character of the cyber warfare in terms both the networks and human factors. A key point he made was that all modern platforms are networks of computers which are vulnerable to cyberattacks. He also defined the future warfare, compared to the contemporary one, as different, computer and network assisted, and combined with cyber campaigns against the population and critical infrastructure of the target nation. Mr Shaffer outlined the mission and activities of NATO STO and the CSO, defining latter as a collaborative production engine of the STO. He also outlined the mission of HFM Panel and the collaborative program of work in cyber domain and the current HFM 288 RWS. His final conclusions about the human factor in building a robust cyber security and defence systems were: training humans to detect the anomalous behaviour and develop better training measures; implement more robust cyber hygiene; evaluate cyber architecture; and incorporate / develop artificial intelligence tools to detect/turn off attacks. The key message of Allan was that any collection of computers in a network is vulnerable and needs a robust protection with humans in the loop. His presentation generated great interest and many questions.

Professor Alan Brill highlighted in his keynote address that cyber offensive operations, if not confronted, have a potential to kick humans out of the loop in cyber security.[2] He discussed the sensitive issue of judicial aspects of cybercrimes, insisting that only humans can be committed to such crimes. He also stressed the requirement for using cyber defence automation and even Artificial Intelligence (AI) cybersecurity tools under human control in successfully protecting against fast automated and sophisticated cyberattacks. Alan claims that the human control must prevent the violation of laws, so “humans have to be in the loop.” His understanding is that different categories of people, working for the offensive or the defensive side of the cyber space, can be the part of the loop and the lines are often blurring. He left three important messages: automated response to cyberattacks will be required but under human control; a formal process for security evaluation of all Internet of Things (IoT) devices need to be established and applied when we buy them; and apply the knowledge of this workshop to our organizations.

Second Keynote session

The second session of the workshop began with two additional keynote presentations. Professor Max Kilger has an extensive experience in the area of information security, especially on the social and psychological factors motivating malicious online actors, hacking groups and cyberterrorists. His presentation highlighted some theoretical work and empirical research into the social processes that shape significantly the threats in cyberspace. He presented some examples of these social processes at the individual, group and global community levels. Max also emphasized the importance of developing a more comprehensive understanding of the relationship between individuals and digital technology as a method for developing future threat scenarios to inform policy makers and defence strategists. His recommendations in this respect, including the incorporation in the scenarios of psychological and social factors, can be considered as a valuable activity for researches and professionals in this area. He underlined the reactive nature of current cyber defence strategies and the necessity for shift to more proactive and preventive strategies. His special emphasis on psychological roots of terrorists' use of cyberspace is of particular value in understanding their motivations and the emergence of cyber terror community. He stressed that the motivations are "the most traditional cause for terrorism and cyberterrorism." A special interest provoked his views on the evolution of cyber communities in the digital world, from hacking through cybercrime to cyber terror community.

Professor Corrado Jiustozzi addressed the issue of the cyber threats in perspective. From historical perspective he stressed the tremendous expansion of Internet with 3 billion users in 2015, and the prediction is to reach 4 billion users in 2019. He presented data of what happened in Internet for 1 minute in 2017: 156 million emails sent, 16 million text messages, 4.1 million videos viewed, 3.5 million Google search queries, 900,000 Facebook logins, etc. He also stressed that in 2019 network connected devices will number more than three-and-a-half that of the Earth population. To his understanding this unmanageable internet complexity created "cultural, behavioural and legal problems in the human society." Corrado believes that exploiting technical, complexity and human/behavioural weaknesses of the cyber space, cyber attackers will always put at risk and compromise cyber security systems. His key message was that in a highly populated cyber space the threats are rapidly growing, as well as the cyberattack surface.

Cyber Resilience: Individual and Organizational Aspects

The three papers in the third session continued the discussion of the key role of human factors to the cyber resilience. LTC Kozok discussed the sensitive topic of insider threats which can be actors, targets and victims. As a target the humans in organizations is exposed to a number of attack tools and tactics: spearfishing, sniffing, open source intelligence (OSINT), dumpster diving, social engineering, Structured Query Language (SQL)-Injection – able to download of User-ID & cryptic passwords, exploit kits, using "lost" USB stick, etc. Through a case

study, LTC Kozok explained the cyber kill chain to kill a company, using above mentioned cyberattack tools and tactics. He also discussed the specific features of the advanced persistent threat (APT) as a sophisticated cyberattack, which aims to establish an illicit, long-term presence on a network. LTC Kozok using various examples revealed some of social media engineering technics and tactics and its influence on the victim. Special emphasis has been put on the reputation attacks, where the human factor is also a victim. However, there were few comments on the most effective security measures against the insider threats.

Mr John Kendal discussed the issue of ethical boundaries in exploiting individual cyber vulnerabilities. In a broader context this huge issue relates to the relationship between any emerging technology and ethics. The exploitation of the cyber vulnerabilities of humans has a huge impact on individual and collective morale of their families and wider communities. From ethical point of view, through examples he illustrated the blurring of the boundary between acceptable and unacceptable cyber action. Mr Kendal also questioned the legitimacy of promoting fear and anger in families and home communities as well as the ethical effect on the operators when they destroy families' cohesion. Addressing cyber enabled information operations and their potential impact on civilian population, John proposed four key ethical issues for discussion, which do not have easy answers: legal and ethical thresholds, the unpredictability of scalability and automation, acceptability of cyber-enabled information operations, and retaliation and guilt.

Professor Todor Tagarev and his associate Ambassador Valeri Rachev in their presentation analysed the key roles of actual and potential cyber units in military organizations, their operational mandates in this grey zone of conflict, and the potential impact on the military ethos.[3] They also shared ideas on what might be the relevant roles, organization and coordination, and career models in cyber units. Recognizing that there is no widely accepted definition of cyber warfare, prof. Tagarev argued that it is hard to define the features of the cyber worrier's profession, as well as the military's role in cyber security. He underlined the basic difficulties in building and retention of cyber warriors and securing their ethics. Reminding NATO's cyber defence pledge of 2016, prof. Tagarev stressed the priority requirement to allied nations to strengthen the security of national networks and infrastructures, which includes a number of national commitments in policy, resource allocations, education, training and exercises. He proposed creating a national cyber learning environment, ranging from the elementary school level to cyber defence exercise for students. Suggesting an indicative taxonomy of cyber worrier functions, prof. Tagarev highlighted the difficulties in defining selection criteria and testing methods when recruiting cyber warriors and their retention in small countries with low payment rates. The ethical challenge facing the cyber warriors is also an impediment in building a robust cyber force.

Cyber Situation Awareness

The fourth session of the workshop focused on cyber situation awareness and was launched with a presentation by Mr. Salvador Llopis, who initially stressed the existing major gap in Decision Support Systems for Cyber defence visualisation and design of user interface to achieve Cyber Situation Awareness. Then he emphasized Human Factors and human performance as important aspects of the engineering design that shall be validated against technology solutions. Mr. Llopis and co- authors from European Defence Agency proposed an experimental validation framework of visualisation techniques using the Situation Awareness Global Assessment Technique (SAGAT) as a methodology originally developed to assist pilot-vehicle interface designs by providing an objective measure of pilot´s situation awareness. In that respect, a variation of the target audience (operators-administrators and military decision makers) and the operational domain cyberspace will modify some of the characteristics validated in the methodology proposed by SAGAT.

Col. Assoc. Prof. Nikolai Stoianov presented a project under development, abbreviated as CyRADARS (Cyber Rapid Analysis for Defence Awareness of Real-time Situation) under NATO Science for Peace and Security Programme. The stated aim of the project is advancement and development of scientific models, metrics, algorithms, and information technologies that support three levels of situational awareness – perception elements in cyber environment, comprehension of the current situation, and projection of future status of cyber environment. It is believed that it will bring benefits to NATO and partner countries even beyond the life of CyRADARS project. The final goal of this ambitious research project is "to develop theoretical foundations, methods, and recommendations, as well as software tools for Situational Awareness (SA) that will enable, in an almost online mode, friendly security forces to: monitor cyberspace to detect malicious information injections and give timely notification of an information attack and; create conditions necessary for decision making about prevention or timely response to enemy's information injections."

Dr. Margaret Varga and her associates, Dr. Carsten Winkelholz and Mrs. Susan Traeber-Burdin, explored different approaches to human machine interface design that can be developed and applied to the different operational and users' needs, in particular the User Centred and System Based approaches to cyber situation awareness. Via WebEx Dr. Varga presented some research results from the experimentation of user centred approach and its visualization through an integrated user centred dashboard for netflow data, which provides user centred visual analytics. The dashboard showed the temporal network situation and threat awareness the network faced. Thus, the users are able interactively and easily to explore the data and gain awareness of the situation. The user centric approach has been developed for effective detecting and discovering cyber threats and its visualization provides sufficient detailed information on the network components (IPs, ports, protocol, etc.), but it does not provide a picture of the operational status of the network. Margaret presented another approach which is suitable to fill this gap, namely the system-based approach,

such as the Ecological Interface Design (EID). It is an interface design for complex socio-technical, real-time, and dynamic systems, which help analysts to see the operational aspects of the network, i.e. the big picture. Thus, the two approaches complement each other and provide an overall picture of the network situation awareness, thus allowing the network security operators to make decisions and solve problems.

Assoc. Prof. Dr. Agata Manolova and her associates Poulkov, Tonchev and Boumbarov focused their presentation on the human interactions for self-coordinating and adaptive wireless Cyber Physical Systems (CFSs) with Human in the Loop. Recognizing the extensive usage of CFSs in many areas, with increased uncertainty of humans in the loop, they have to be predictable and need self-coordination and adaptation. To her understanding such a system must take into consideration human response and presence including gestures, pose, emotional state and behaviour, which becomes a key part of that system. According to Dr. Manolova, such system requires "to develop and integrate reliable and accurate human behaviour modelling techniques that attempt to learn and predict human behaviour." She described a taxonomy of gestures for human-computer interaction and some technology solutions for gesture and emotion detection and recognition. Agata stressed that a number of research challenges have to be overcome to realize such Adaptive Wireless Cyber Physical Systems (CFSs) with Human in the Loop, which could have many practical implications, such as cyber-physical transportation systems, health care and medicine system, home health care platform, cyber physical energy systems, etc. Dr. Manolova concluded that the long-term CPS goal is to transform the way we interact with the physical world as we interact with one another in the Internet.

Innovative Human Systems Integration Approaches to Cope with Cyber Threats

The fifth session of the workshop focused on innovative human systems integration approaches to neutralize cyber threats. The presentation by Mr. Konstantin Zografov discussed the innovative biometric and information technologies for EU border security and global migration control, and their contribution to security and defence. The key point is that the problems with a massive migrant's identity and related crimes with trafficking humans require the digital identity to become a security factor. It is defined as "an online or network identity adopted or claimed in cyber space by an individual, organization or electronic device." Mr. Zografov stressed that it is based on various biometrics and refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. He numbered several types of biometric identification schemes: face, fingerprint, hand geometry, retina, iris, signature, vein, and voice. The successful use of biometrics led to the development and field testing of UNHCR's new biometric identity management system (BIMS). The application of biometrics is also expanding in many other areas.

Professor Alfredo Ronchi continued the discussion on the border control, focusing on the issue of trust assessment systems, based on risk analysis and clus-

tered sensors. The general description of the system logic and architecture introduces the core of the solution – the Trust Assessment System (TAS) that predominantly takes into account the human factors.[4] Its primary objective is to provide the border control authorities with enhanced situational awareness, and capabilities for timely and proper identification of potentially dangerous people and goods, thus preventing smuggling and human trafficking. According to professor Ronchi, main benefits of such systems include: improved checkpoint throughput, improved level of security, better traveller experience, and optimisation of resources. He stressed one key aspect of TAS namely change border crossing point paradigm from the current "check-everything-at-the-border" to the more efficient "check-everything-till-the-border." This solution fits mainly with border crossing points but it is not limited to this sector, it may be used in a number of different situations, outlined in the presentation.

Dr. G. Scott Knight, addressed the audience on a very sensitive issue associated with the weapon systems cybersecurity, taking as an example the avionics cybersecurity. His presentation reflected the recognition that the avionics as well as weapons embedded in the military aircraft and other platforms are vulnerable to cyberattacks and need to be protected. On the base of cyber kill chain model, he described all possible steps for cyber penetration and malicious exploitation of aircraft avionics which could affect mission implementation even to cause downing of aircraft. Cyber-affected avionics could also potentially affect broader platform-linked systems, as well as national or NATO integrated air and missile defence system. To counter weapon systems cybersecurity threats Dr. Knight emphasized that a robust network defence has to be established, able to respond to each phase of the cyber kill chain, from reconnaissance to actions on objectives, thus detecting and responding to each malicious action. The presentation attracted the attention of the audience and raised several questions.

Cyber Security Education and Training

The four presentations in the sixth session of the workshop focused on the importance and various approaches to cyber security education and training. The presentation by Dr. B. Jekov and his associates Prof. E. Shoikova, Prof. E. Kovacheva, Assoc. Prof. R. Nikolov addressed the issue of development of a competence-based curriculum in cybersecurity. He presented three subtopics: strategic plan of the State University for Library Studies and Information Technologies (ULSIT) initiative for cybersecurity education; framework for planning, design and implementation of Competence-Based Education (CBE); ULSIT projects of competence-based cybersecurity education and training. The vision, mission and goals and objectives of ULSIT's initiative for cybersecurity education indicate that a comprehensive approach is applied to achieve a credible and effective cybersecurity education, aimed to produce knowledgeable and skilled cybersecurity workforce. Dr. Jekov also stressed the key characteristics of the CBE, namely: learner-centric, outcomes-based, and differentiated (to meet the needs of individual learners). Finally, Dr. Jekov briefly described the ULSIT's pro-

ject for competence-based cybersecurity education and training, developed within the framework of EU ERASMUS+ programme, in cooperation with Moldova, Kazakhstan and Vietnam.

The presentation by Dr. Jorge L. Hernandez-Ardieta and Professor Juan Tapiador discussed the topic on the adaptive cybersecurity training in cyber range environments. Due to vast cybersecurity workforce shortage in the coming years, he claimed that cybersecurity training and education (T&E) has become a pillar in any cybersecurity strategy. In his understanding, despite thousands of courses and hundreds of centres of excellence for cybersecurity in many countries and international organizations, satisfying specific needs is still insufficient and achieving proficiency in cybersecurity is a difficult, expensive, and time-consuming. Current cybersecurity T&E models have a number of limitations. Dr. Hernandez sees a promising solution in this regard, which is a project under development – Cyber Range. It is defined as a "technological platform for hands-on training, technology experimentation and research in cybersecurity," built on a virtualization technology and is regarded as an effective approach to build enhanced, tailored, and cost-effective cybersecurity training for large scale audience.

Dr. Bistra Vasileva provided a current overview of the existing body of the literature in the field of cyber security education and required digital competences. The author's main objective is to develop a reference framework of digital competences which will provide students or trainees the opportunity to acquire knowledge and skills to deal with different situations of cyber threats. She proposes a holistic educational approach, able to integrate formal, non-formal and informal education and its core is simulation-based learning. This approach focuses on the development of three groups of skills: cognitive, decision making and tactical abilities. The objectives of her comparative study are: to identify the critical digital competences needed for ensuring cyber secure behaviour; to conduct a comparative research; and to propose a reference framework of digital competences about cyber security.

Mr Oleg Chertov and his associates Taras Rudnyk and Olexandr Palchenko addressed in their presentation the growing impact of the fake information in social networks. The goal of their research work is to detect phony accounts and fake information on Facebook. During their research, they have identified a number of interesting factors that allow us to understand goals of people that use fake information. Their hypothesis was that "phony accounts firstly try to get smashed in confidence and wait for right time to spread lies." The experimental results supported hypothesis by showing that such phony accounts were found in pages of some Ukrainian politicians.

Cyber Security: How to Improve Human Machine Interface?

The seventh session of the workshop was dedicated to the human-machine interface in the cyber security. The first presentation by Dr. Veronica Wendt was directly linked to the session topic. Highlighting the human, machine and computer strengths, she stressed that "the improvement of human-machine inter-

faces necessitates new processes." Strengthening cybersecurity through improved human-machine interfaces can be achieved by identifying the human "pain points" in the cybersecurity ecosystem, analysing which of them can be replaced by machines, and then developing new processes to take advantage of the shifting roles. The key point she made was that as the roles between humans and machines shift, the value would be in the development of the new processes and the ability to scale and replicate those same processes. The recommendation of Dr. Wendt for a process change was "to examine current and experiment with new processes."

Dr. Olexandr Burov proposed in his presentation a review of cyberspace vulnerabilities and cybercrimes. On this basis he promoted a cybersecurity model (CSM) for humans as subjects, objects and threats in network-depended activities. Dr. Burov discussed challenges provoked by digital space in relation to influential factors, ways of their avoiding and appropriate tools. His analysis is based on experience of human factors/education findings for adults (emergent and military operators) and features of cognitive abilities of high school students. He also introduced the ideas about cognitive weapons, as well as of a cognitive war which is emerging as a new type of war. He claimed the aim of latter is "implanting to the enemy a thought that the struggle itself does not exist" thus leading to the self-destruction of the opponent nation. In his understanding the cognitive damage is realized through introduction of false theories in the science and education, which also influence expert society, government and decision makers, public policy and management' The final outcome is the weakening of national resilience and defence potential.

Assoc. Prof. Dr. Zlatogor Minchev focused his presentation on the role of human factor in proactive cyber defence, defining it as ambivalent. Describing today and future cyber realities, he highlighted some challenges and changes in human-machine-environment interaction. In the search to cope with these challenges proactively, Zlatogor presented a research methodology with an algorithm of four stages: threat landscape definition, system modelling and analysis, hybrid (human-machine) simulation, and results validation & verification. Thus, he outlined a comprehensive methodological outlook for system-of-system foresight analysis, on the basis of expert and reference data for future cyber threats & risks analysis. He also provided additional probabilistic results, computational validation and human-factor multimodal verification. The research results have been successfully implemented for both national and international high-level future strategic analyses & assessments for the integrated security sector. He also informed about Secure Digital Future 21 initiative established in Joint Training Simulation & Analysis Centre to the Bulgarian Academy of Science. His final conclusion was that cyber-physical co-existence is dynamically transforming and leading to change in human-machine-environment interaction, respectively to the role of the human factor.

Vulnerabilities with Respect to the Role of Human Factors and Organizational Processes in Cyber Defence

Under the theme of the eighth session four papers and presentations introduced vulnerabilities in cyber defence, based on the role of human factors and organizational processes. The presentation by Assoc. Prof. Dr. Velizar Shalamanov is a part of the study on best practices for management of IT organizations for effectiveness, efficiency and cyber resilience. Key processes are assessed from the organizational cyber risk prospective as a base to define model for the organizational aspects of cyber resilience as well as the role of human factor. Using this model, developed for crisis management domain, he has adapted it in support of organizational / human risks in cyber domain and to support research and training for cyber resilience. This environment BEST-Cyber (Basic/budget Environment for Simulation and Training) is used for PESTEL (Policy, Economic aspects, Social dimension, Technology aspects, Environment, Legal issues) analysis of cyber environment in organization to identify model for resilience from organizational/human perspective.

Br. Gen. (ret) Antonio Trogu defined in his presentation the centrality of the human factor as main cyber defence and prevention tool. A key point he made was that the cyber security mission will require a workforce with enhanced skills for ensuring the security of the national critical infrastructure. Assessing the cyber threats trends and actors involved in the formulation of cyber policies, he underlined that each nation should "develop and maintain expertise in all matters related to cyber defence." Gen. Trogu has also shared information about the creation of the Italian Joint Cyber Command which will achieve full operational capability in 2019. His final point was that the human factors are the biggest challenge in building an effective cyber threat prevention strategy.

Ambassador (ret.) Dr. Peter Popchev addressed an important issue for developing a holistic cyber security and cyber defence strategy by collaborative efforts of NATO and EU, through a doctrinal alignment and structured coordination.[5] Outlining the characteristics of the typical hybrid warfare, its scope and goals, he emphasized the critical role of the AI as a game-changer. His concern was that the co-evolution of AI, machine learning and cybersecurity may question the place of human in the loop. On the basis of the nature, scope and goals of the current and future cyber threats, he outlined the general direction, stages and principals of possible NATO-EU cyber security & cyber defence strategy. In his understanding this three-stage collaborative work should result in a draft strategy to be sent to governments. At the end of his presentation he identified several principles of such strategy and the key principal is the "central stage" of the human factor, which requires "a new approach to education, learning on the job, selection, academic and industry exchange…," to mention few of them.

Lessons learned and Future Research Perspectives

In the last session of the workshop three papers addresses the issue of the lessons learned and future research perspective on the broad theme of the human systems integration approach to cyber security. Mr. Atahas Radev addressed

cyber security from the perspective of Internet user ethics and cyber protection habits. To his understanding, the Internet user ethics is based on a set of moral principles that govern an individual or a group on what is acceptable while using internet, meaning one should respect the rights and property of others on the web (internet). His presentation was focused on the intentions of people as users, both at work and outside, and their noble or malicious behaviour. To author's opinion, Internet user ethics must to be considered as a code of behaviour for moral, legal and social issues on the Internet, based on several moral principles: acceptance, sensitivity to national and local cultures, using e-mail and chatting, not pretending to be someone else; hiding your personal information, respect the copyrighted materials of others, avoiding bad language, to mention few. Mr. Radev numbered several basic protection habits, which every Internet user should comply with.

Dr. Arnold C. Dupuy (via WebEx), addressed the nexus between cybersecurity and operational energy to support the warfighter in every operation. This is a critical issue for the U.S. Department of Defense, which is fully dependent on both the cyber and energy infrastructures in the conduct of global operations. In particular, the presentation discussed the cyber environment in the operational energy space, the existing vulnerabilities in the intersection between cybersecurity and operational energy and some current and future mitigation strategies to address this growing problem. Operational energy is regarded as a "fundamental enabler of military capability" and energy requirements are increasing, which brings also increased risk. In the US departments of defence and energy engineers and policy analysts have formed a research group to examine the growing cyber threat to the critical infrastructure with focus on the energy sector. This effort, called MOSAICS (More Situational Awareness for Industrial Control Systems), has received official recognition from two strategic commanders (PACOM and NORTHCOM).

Dr. Natalia Derbentseva, a member of NATO STO HFM 259 RTG "Human Systems Integration Approach to Cyber Security," presented the intermediate findings of the research team. She briefly discussed the objectives of 259 RTG, which are entirely focused on the role and place of HF in cyber security and associated vulnerabilities. An impressive amount of work has been done by the research team in the last two years to develop a conceptual framework of human factors in cyber security, data collection, analysis and relational database (MySQL) with a web-based interface application to support data exploration. The overview of the conceptual framework reveals that 25 concepts have been defined, each with multiple levels, describing the conceptual components: threat, affected target, attack outcome, mitigation, and source characteristics. The conceptual framework is visualized as a network with nodes representing concepts. Data collection currently includes 250 open sources (journal articles, books, reports), each coded against each of the 25 concepts. Finally, Dr. Derbentseva outlined the way forward, i.e. the work remained to be done until the end of 2018.

Key messages

In analysing the content of the presentations and taking into account the session discussions, several key messages emerged from the research workshop. The following list provides summary of more significant of them:

- Cyber warfare is changing and becoming more complex and encompassing all state and non-state sectors;
- Nearly all modern platforms are a network of computers with increased vulnerabilities and need a robust cyber protection and defence;
- Unmanned air, land and sea platforms will start to dominate the future battlefield or part of it in next 15-20 years;
- Enhanced and regular cybersecurity training and more robust cyber hygiene is the key to achieve a strong cyber resilience;
- The concept of humans staying in the loop in cyber security and defence, through automation and controlled AI, is recognized requirement to guarantee the effective response to current and future cyber threats;
- All nations and international organizations need to develop proactive cyber security and cyber defence strategies;
- Each government should prevent the evolution of cyber hacking community into cybercrime community and the former into cyber terror community;
- The rapid diffusion of the Internet has created cultural, behavioural and legal problems in the human society, which have to be addressed at national and international levels;
- The expanding complexity of cyber space, if not addressed and regulated, will create cyber chaos with unpredictable consequences;
- Ethical aspects of exploiting individual cyber vulnerabilities generates more questions than answers;
- All modern armies need certain cyber capabilities, depending on their resources and ambitions;
- Cyber warrior's profession requires a specific and flexible recruitment, training and payment to retain in service highly qualified individuals;
- Visualization provides an enhanced support to commanders to achieve Cyber Situation Awareness and to build Proactive Cyber Defence;
- The battlespace is already inside our weapon systems and requires an adaptation of our force structure and force development, and training;
- Competence-based cybersecurity education and training is an innovative approach to build knowledgeable and skilled cybersecurity workforce;
- Cybersecurity training and education (T&E) is a key pillar in any cybersecurity strategy;

- Cyber Range is an effective approach to acquire and enhance practical knowledge, skills, and abilities, and supports massive-scale, tailored, and cost-effective cybersecurity training;
- Improving Human-Machine Interfaces (HMI) necessitates new processes, based on the examination of current and experimentation of new processes;
- Cyberspace vulnerabilities are expanding and leads to cognitive war, which is programming cognitively the opponent to self-destruction;
- Solid design, professional institution building and change management are essential for the cyber resilience of IT organizations;
- The human factor is becoming the dominant prevention tool in cyber security and cyber defence;
- The mitigation of Operational Energy Cyber Mission Risk is of a key importance in both of civilian and military operational spectrum.

Conclusions and Recommendations

The growing complexity of cyberspace and cyber threats requires an integrated approach to cybersecurity and defence, involving not only technology but also humans on equal basis. Until several years ago the role of humans was underestimated or even neglected. When it became evident that most of security breaches in the cybersecurity and defence systems are due to human errors the paradigm started to shift. The general idea behind the concept "Human in the loop" is to build "a human wall" in each resilient cybersecurity and cyber defence system. The concept reflects the critical role and responsibilities of human factor in preventing and defending against cyberattacks in their various forms. The education and training of humans for responsible behaviour in the cyberspace is a key effort in many public and business national and international organizations, and is expanding in the recent years. The theme of HFM – 288 RWS reflected this trend and overall requirement. All nine topics suggested in the workshop concept have been relatively well covered in the presentations and associated discussions. Additional topics complemented the list and highlighted additional aspect of the workshop research theme. Most of the presentations generated an enhanced interest and provoked a number of questions. However, some presentations were not directly linked to the session topics but highlighted additional aspects of the cybersecurity. Most of the presentations bound and complemented various aspects of the role of the human factor in the integrated approach to cyber security and cyber defence. In few sessions very limited time was allocated for discussion. More attention should be given to the use of Artificial Intelligence in building robust cybersecurity, while ensuring a human control over this technology. The issue of Human-in-the Loop Cyber Physical Systems (HiTLCPS) also requires more research due the development of future HiTLCPS with stronger ties between humans and control loops. During most of the sessions there was a valuable exchange of views and suggestions,

which provided a basis for the technical evaluator to derive several recommendations for NATO and partner nations, concerning the human factor in the integrated approach to cyber defence. Following is a short list of more important of them:

- NATO STO should develop and maintain more expertise in all human matters related to cyber security and cyber defence;
- More exploratory efforts are needed on the prevention tools to the exploitation of human/behavioural weaknesses in cybersecurity and defence systems;
- More research is required in the domain of Human-in-the Loop Cyber Physical Systems and its security implications;
- NATO STO should encourage academic research targeted at effective and validated Modelling and Simulation of human cognitive processes and behaviour in cyber domain with focus on human factors in the models;
- NATO, allied and partner nations need to explore all aspects of the Human Control over the Artificial Intelligence, used in cyber defence, command and control, and weapon systems;
- More research is needed on the human cognitive process of the cyber situation awareness.

In summary, the workshop achieved its goals. Many concepts, approaches, tools and techniques associated with the role of humans in building and sustaining resilient cyber security and cyber defence systems were exposed, and various lessons learned were discussed. The research efforts on the role of humans in fighting the rapidly expanding cyber threats should continue, as the cyber domain is becoming critical for the success in the future battlefield.

References

1 Yantsislav Yanakiev, ed., *Proceedings of International Conference "Human Systems Integration Approach to Cyber Security"* (Sofia, 2016).

2 Alan Brill and Jonathan Fairtlough, "Fighting the First Battle of Cyberspace Preparedness: Finding Your Reserve Cyber-Warriors," *Information & Security: An International Journal* 44 (2020): 9-15.

3 Todor Tagarev and Valeri Ratchev, "Cyberwarriors: The Backbone of the Future Military or a Misnomer?" *Information & Security: An International Journal* 44 (2020): 17-26.

4 Alfredo M. Ronchi, "TAS: Trust Assessment System," *Information & Security: An International Journal* 44 (2020): 62-75.

[5] Peter Poptchev, "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages," *Information & Security: An International Journal* 45 (2020): 35-55, https://doi.org/10.11610/isij.4503.

About the Author

Sabi I Sabev is a retired Major General in the Bulgarian Armed Forces. During his active duty service, MG Sabev has been involved in the development of the operational capabilities of the Bulgarian Armed forces and its organizational structures. He has headed key staff structures of air regiment, division and corps, within Air Force HQ and General Staff of the Bulgarian Armed Forces. He has been heavily involved in the elaboration of strategic reviews, analyses and plans, strategic and doctrinal guiding documents, planning and participation of Bulgarian military contingents in NATO and PfP exercises and peacekeeping operations. As the first National Military Representative to NATO HQ after the accession to NATO, he has built up and integrated the Bulgarian military representation into NATO Military Committee activities.

After his retirement in 2005, he worked for the Defence Advance Research Institute of Rakovski National Defence College of Bulgaria. He was also a lecturer in New Bulgarian University. His expertise is in the areas of NATO and EU security strategies, military strategies and doctrines, national and Alliance defence and force transformation initiatives, defence studies for the Balkans and the Wider Black region.