Information & Security

Y. Yanakiev & D. Polimirova
vol. 44 (2020): 39-50
https://doi.org/10.11610/isij.4404

Published since 1998

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

Research Article

Exploring the Role of the Human Factor in Cybersecurity: Results from an Expert Survey in Bulgaria

Yantsislav Yanakiev [1] (✉), *Dimitrina Polimirova* [2]

[1] *Defence Institute "Prof. Tsvetan Lazarov", Sofia, Bulgaria, https://di.mod.bg*

[2] *National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Sofia, https://nlcv.bas.bg*

ABSTRACT:

This article presents results from Subject Matter Experts' opinion survey carried out by the authors in Bulgaria and aimed at obtaining and summarizing the widest possible range of information on issues related to the challenges of ensuring cybersecurity in the country, including the important role of human factors in cybersecurity. The survey was carried out in the framework of a project funded by the Bulgarian Institute of Public Administration in 2019. The questions included in the survey relate to three distinct sectors—the public administration, academia and the business sector—all contributing to the operational support of the e-government in Bulgaria; the consolidation of this support is seen as prerequisite for achieving a cyber sustainable Bulgaria. The results of the survey are intended to support the process of formulating conclusions and recommendations for improving decision-making regarding the role of the human factor in cybersecurity in the public administration of the Republic of Bulgaria, enhancing the institutional capacity, recruitment, development and retention of IT personnel.

ARTICLE INFO:

RECEIVED: 19 OCT 2020
REVISED: 22 NOV 2020
ONLINE: 30 NOV 2020

KEYWORDS:

cybersecurity, human factors, recruitment, retention, education & training, IT personnel

✉ Tel.: +35929221662; Fax: +359292808; E-mail: y.yanakiev@di.mod.bg

Introduction

While technological solutions are being developed to enhance cybersecurity, there is growing awareness that besides a technical approach, the role of human performance, decision-making, education and training and organisational culture are critical to foster the effectiveness of responses to developing cyber threats.[1, 3, 4, 5]

Current studies show that the human factor may be a system's 'weakest link,'[8] but may also be a powerful resource to detect and mitigate cyber threats.[9, 10] In the same time, the variety of human factors involved in cyberspace and the absence of a consistent theory seem to hinder the focused development of integrated approaches to cybersecurity. Moreover, there is a lack of research attention devoted to the role of organisational culture and processes to increase cybersecurity capacity. Finally, further research is needed to improve the state of cybersecurity education, training, exercises, and evaluation, plus identifying specific lessons that we are learning in both training and operations. To summarize, the challenge for both collective and national security is to minimize the risks of cyber as a threat.

The NATO Policy on Cyber Defence[6] posits that cyber defence is part of the Alliances core task of collective defence, confirms that international law applies in cyberspace and intensifies NATOs cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance. Besides, the European Union Cybersecurity Strategy: An Open, Safe and Secure Cyberspace[2] also defines the cyber threat among the most important for the EU and its Member States (MS).

Recent publication of NATO Science and Technology Organization (NATO STO) identified several areas of most critical and urgent needs and the knowledge gaps to address in cyber research agendas of NATO and the nations that can be defined as Psychosocial, Cultural, Conceptual and Organizational dimensions of cybersecurity. The common perspective for these research needs is that the interaction between users, cybersecurity specialists, interconnected organisations, and technologies form a sociotechnical system that balance security needs with operational needs.[7]

Among the most urgent human factors needs that require further collaborative research are the following: (1) Approaches to improve selection, education, training and retention of a cyber force (IT experts); (2) Approaches to improve cyber awareness and cyber hygiene of all defence personnel; (3) Practices to enhance organizational resilience to cyber-attacks; (4) Methods to improve control behaviour via cybersecurity policies and targeted Education and Training (E&T).[7]

Taking into account the identified human factors related issues of cybersecurity at NATO level, the authors initiated a Subject Matter Experts (SMEs) survey in Bulgaria aimed at obtaining and summarizing the widest possible range of information on issues related to the challenges of ensuring cybersecurity in Bulgaria, including the important role of human factors (HF) in cybersecurity.

Among the topics that cover HF domain are the status and the development of human resources in the cybersecurity, what is SMEs views about the process of recruitment, training, motivation and retention of cyber warriors, how they see future research needs in the area of human factors in cybersecurity, etc. The paper presents a summary of the obtained results and some ideas for minimizing the vulnerabilities due to the HF.

The results of the SMEs survey should support the process of formulating conclusions and recommendations for improving decision-making regarding the role of HF in cybersecurity in the public administration of the Republic of Bulgaria, improvement of institutional capacity, recruitment, development and retention of IT personnel.

The questions included in the survey concern the three sectors—public administration, academia and business sector—as participants in the operational support of the e-government in Bulgaria, whose consolidation is a requirement for achieving a cyber-sustainable Bulgaria.

Method

The methodology for data collection includes self-reporting online questionnaire. The link to the questionnaire was sent to 369 people in the state administration, 121 representatives of academic organizations and 95 business organizations. The response rate was 10.7 % which means that 92 participants from the three sectors were active and filled out the questionnaire.

The questionnaire contains 50 questions, which are grouped into five main sets, concerning:

(1) Current state and development of human potential in the cybersecurity domain;

(2) Current conditions of the equipment and resources of cybersecurity specialists;

(3) Cybersecurity management and policies;

(4) Interaction between the three main sectors: state, academia and industry;

(5) Innovative technologies for cybersecurity.

This paper focuses only on the responses of the SMEs related to the role of HF in cybersecurity.

The positions of the respondents can be divided into three main groups: (1) managerial; (2) expert and (3) research. The predominant part (85 %) of them consider that they have a level of expertise in cybersecurity issues, sufficient for the needs of the organization, good and high. They believe that only 15 % of cybersecurity staff have a low level of expertise in the cybersecurity domain.

Results

The Most Important Cybersecurity Issues in Bulgaria and the Role of Human Factor

According to the received evaluations of SMEs, the most serious problem of cybersecurity in Bulgaria is the insufficient capacity (knowledge and skills) of IT staff. Nearly two-thirds of the experts (64 %) identify this issue as problematic (Fig.1).

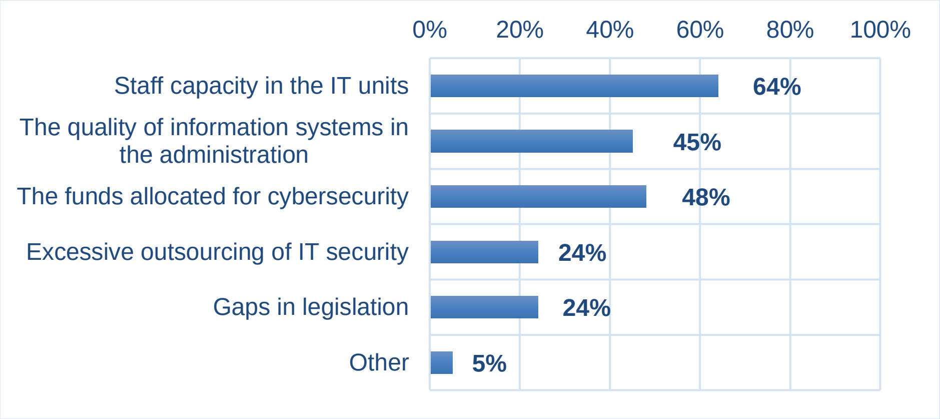

Figure 1: Distribution of the answers of the SMEs to the question "Please indicate and justify the three most important current problems in the field of cybersecurity in Bulgaria."

On the second place as a problematic issue, almost half of SMEs (48 %) identified the insufficient funds allocated for cybersecurity. The third important badly-behaved issue is the quality of the information systems in the State administration, recognised by approximately half of the experts (45 %). At the fourth place SMEs, recognize some gaps in the regulatory framework and the practice of excessive outsourcing of IT services, in some cases leading to poor quality of cybersecurity. This opinion is supported by approximately a quarter of the SMEs (24 %). The same is the percentage of SMEs who think that there exists a practice of excessive outsourcing of IT services. Single experts believe that there is a lack of understanding among management of the organisation that the problem is downplaying or that work is being done piecemeal.

The percentages presented in the figure do not sum up to 100 % because the respondents had the opportunity to indicate each correct answer.

In agreement with the definite opinion of the SMEs about the key role of HF in cybersecurity, they consider that it is necessary to pay special attention to the role of the human factor in the field of cybersecurity in Bulgaria (Fig. 2).

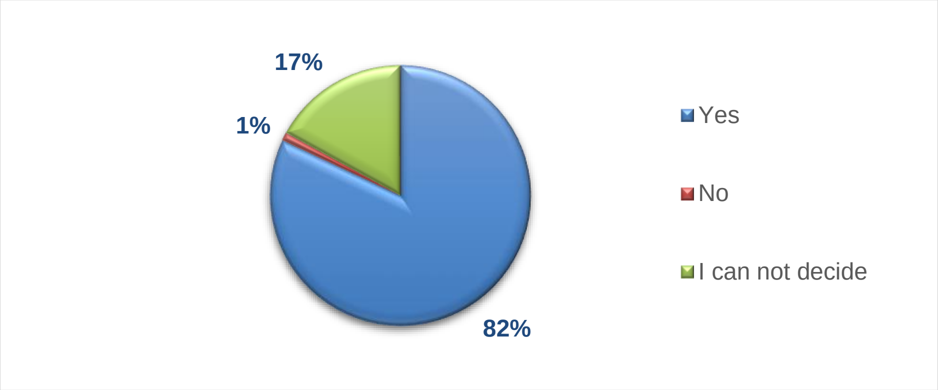

Figure 2: Distribution of the answers of the SMEs to the question "Do you think that it is necessary to pay special attention to the role of the human factor in the field of cybersecurity in Bulgaria?"

Again, the vast majority of the experts emphasize the key role of the human factor in cybersecurity. Significantly, only 1 per cent indicated that it was not necessary to focus on the role of people in preventing cyber incidents, raising general awareness and responding adequately in the event of a threat. The main recommendations of the experts express in the open questions are:

- "Need of a long-term strategy for ensuring the necessary human potential";
- "Selection, training, certification, rotation of IT personnel between public administration, industry, academia, NATO and EU, loyalty check";
- "It is important to assess the behaviour, attitudes and moods of the users in cyberspace to anticipate their actions and expectations";
- "Cybersecurity technologies have a very short life cycle. They can be acquired relatively quickly and easily. It is difficult to build and develop human potential. We need to determine what specialists we need to ensure a healthy surplus of specialists in each specific area of cybersecurity";
- "The human factor is the riskiest; it is a part of the system; basic vulnerability even in the most secure systems";
- "As the weakest link in any organization, HF requires special attention, especially in terms of training to increase the competencies of employees and compliance with good practices in the field of cybersecurity."

Recruitment, Retention, Education & Training of IT personnel

The vast majority of experts (70 %) believe that changes are needed in recruitment, education, training, retention and lessons learned from cybersecurity practice (Fig. 3). Just 3 % of the people consider that such changes are not necessary and a quarter (27 %) cannot express opinion probably because they have

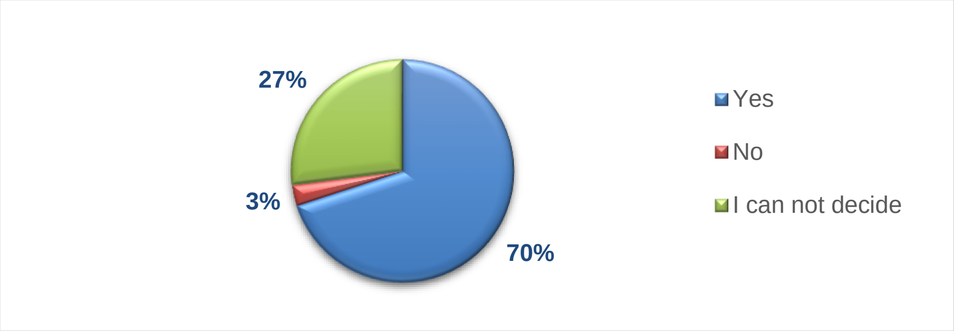

Figure 3: Distribution of the answers of the SMEs to the question "Do you think that there is a need for change in the recruitment, education, training, retention and lessons learned from the practice in the field of cybersecurity in Bulgaria?"

no experience in the field of recruitment, education, training, retention and lessons learned.

It is important to present some specific proposals again based on the SMEs responses to the opened questions:

- "They (IT experts) must complete certifications for this, and have such a speciality in technical higher education institutions";
- "The staff should be recruited according to the specific task, and not to be Swiss Army knives";
- "It is fashionable to teach cybersecurity to people who have never worked in this field. There are no clearly defined abilities that are being built. Training is not provided with high technologies and platforms. The lectures, which are borrowed from western and eastern sources, are not provided with the possibility for practical work and verification. Investments, to put it mildly, do not achieve their goal, which speaks of their misdirection";
- "Establishment of specialized training and "on-site" units";
- "Focus on training and retention".

Besides, in a series of questions, experts were asked to indicate whether changes are needed in the regulatory framework, strategies, concepts, doctrines and organization of the cybersecurity system. In most cases, over half of those surveyed indicated that such changes were necessary. Also, they give specific suggestions on what to change. Here are some examples:

- "Procedures for interaction between organizations";
- "Clear rules for the public-private partnership";
- "Doctrinal issues for cooperation within NATO and the EU";
- "Procedures for action in different scenarios. Procedure for review and update of the cybersecurity strategy";

- "There must be clearly defined as individuals, teams and responsibilities. To set goals for them. In case of failure to achieve the goals - to have changes in the teams. In this way, in a relatively short period, working teams will be formed and the state administration will get rid of non-working structures and pseudo-experts".

Even though most of the experts consider very important to have specialized education and training for the people in the organization to increase cybersecurity awareness, the survey shows that in most cases (59 %) such training have not been conducted (Fig. 4).

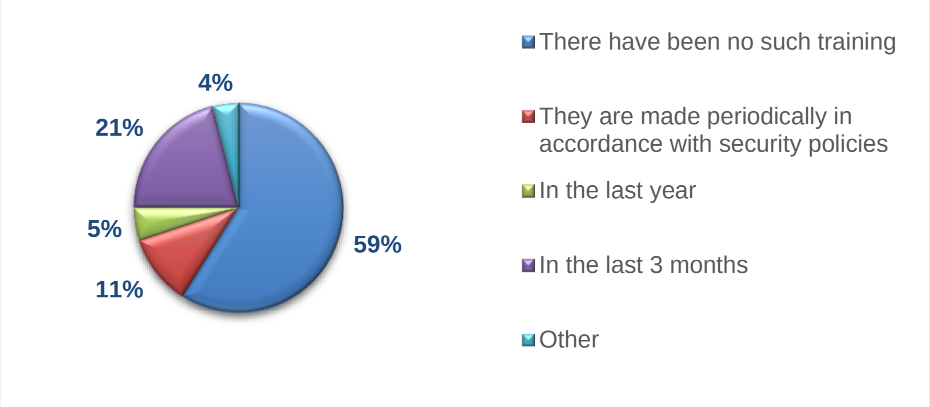

Figure 4: Distribution of the answers of the SMEs to the question "When was the last training on cybersecurity in your organization?"

One-fifth of the experts (21%) say that cybersecurity training has been done over the last three months and 5 % – over the last year. Besides, 11 % of them think that training has been organized periodically according to their needs and cybersecurity policies. Finally, 4 % of SMEs give other answers such as:

- "3 years ago";
- "In the last 6 months";
- "Currently in progress";
- "Such training is conducted only for the administrators of information systems."

The Human Factor as a Source of a Cybersecurity Breach

The data received from the SMEs demonstrates that most of the cases of cybersecurity breaches are related to human error or another HF vulnerability (Fig. 5).

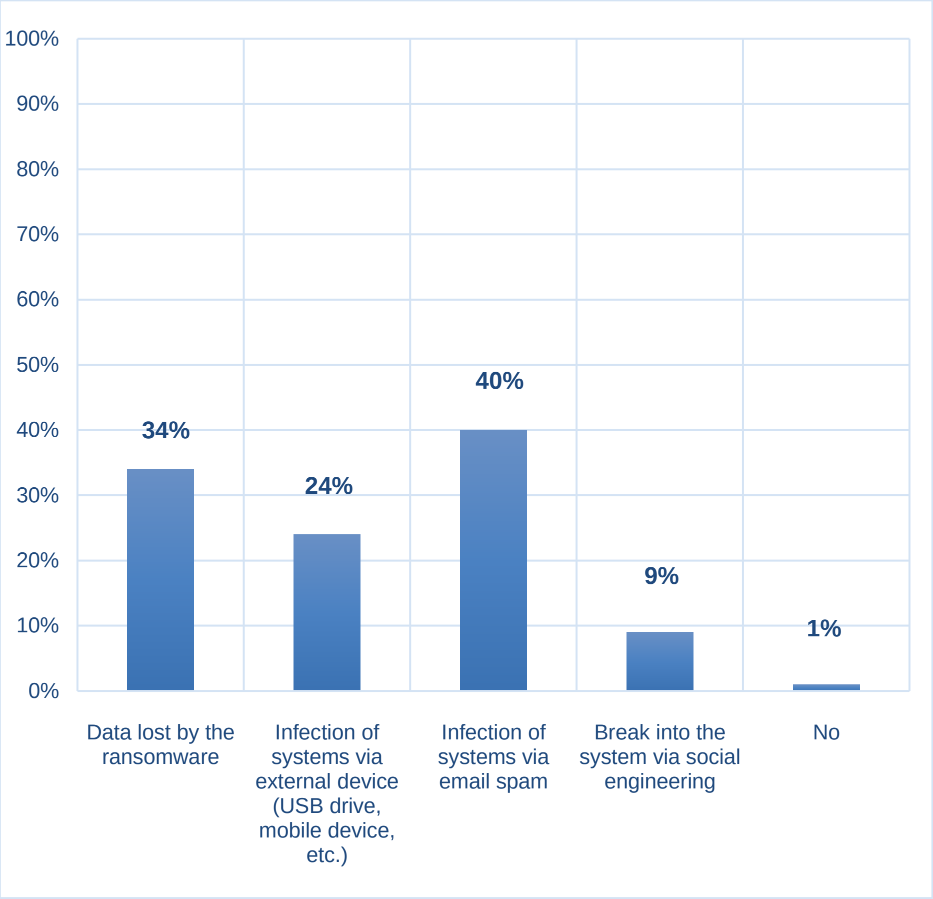

Figure 5: Distribution of the answers of the SMEs to the question "Did your organization has encountered any of the following problems?"

There is more than one answer to this question. The most common problems related to successful attacks are spam and ransomware. Again, the data clearly shows that most of the dangerous and hostile attacks are related to HF vulnerabilities (Fig. 6).

Here, the respondents can give more than one answer. Most of them believe that the most dangerous and hostile type of attacks are data theft in any form, violation of the physical integrity of systems and networks and targeted attacks. Other answers (12%) includes:

- data encryption (ransomware);
- spam attacks;
- Phishing attacks.

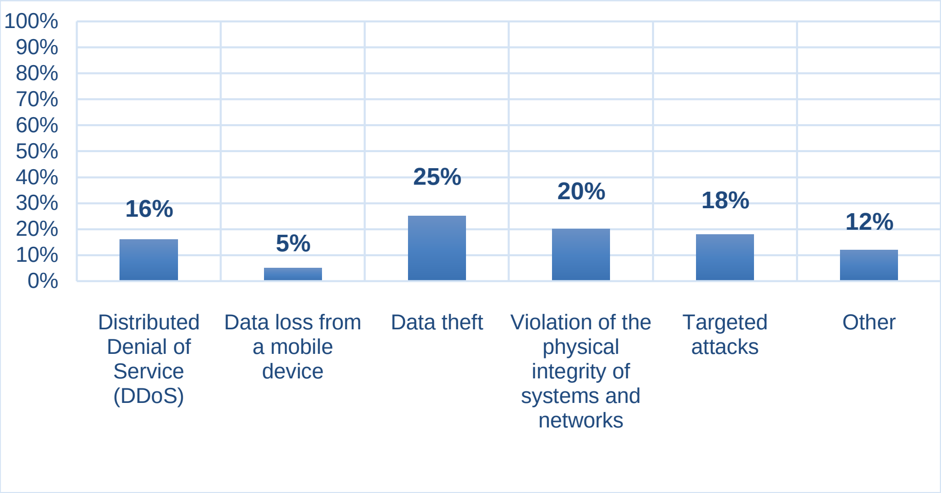

Figure 6: Distribution of the answers of the SMEs to the question "Which are the most hostile type of attacks?"

Future Research in the Area of Human Factors in Cybersecurity

Obviously, there is a great need for future research in the area of HF as an important part of the socio-technical system of cybersecurity (Fig. 7).

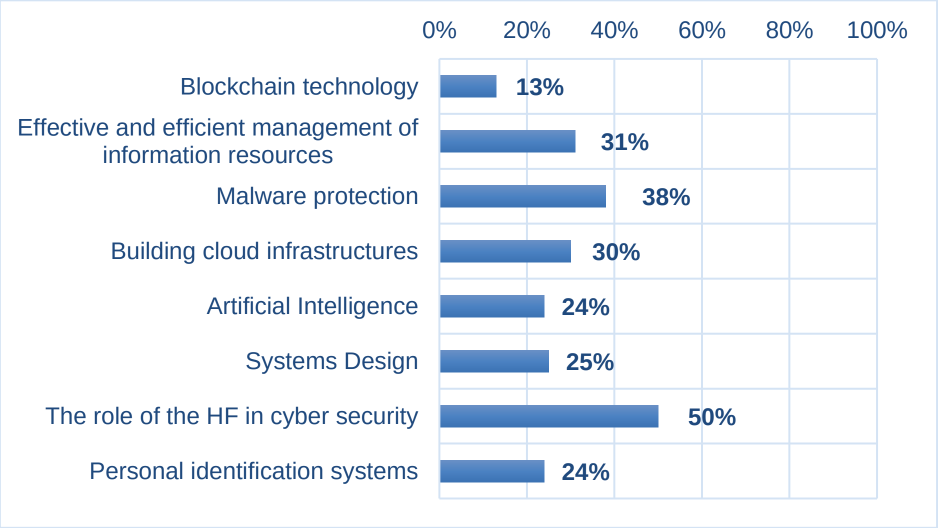

Figure 7: Distribution of the answers of the SMEs to the question "Please indicate and justify what you consider to be the three most important areas that require research in the field of cybersecurity".

Respondents had the opportunity to indicate each correct answer, and therefore the sum of the percentages exceeds 100 %.

The role of the human factor in cybersecurity is indicated with the largest share of answers, as an area in which there is a need for further research (50 %). Experts definitely believe that an integrated approach to cybersecurity is needed, which should include the human at the centre of the socio-technical system, together with new technologies, software innovations, organizational and regulatory changes, etc. Also, protection against viruses and malware, effective and efficient management of information resources and the construction of cloud infrastructures are identified as important research areas. The third group of areas in need of further research in Artificial Intelligence, systems design and personal identification systems. Interest in blockchain technologies is relatively lower, probably due to their lower popularity.

Conclusions

This article focuses on the viewpoints of the SMEs in cybersecurity in Bulgaria about the process of recruitment, training, motivation and retention of IT experts, as well as their opinions about future research needs in the area of human factors in cybersecurity.

Our data confirmed the general thinking of the expert's community that the human factor may be the 'weakest link' in cybersecurity as a socio-technical system. Therefore, the experts think that most of the cases of cybersecurity breaches are related to human error or another HF vulnerability. The most common problems related to successful attacks are spam and ransomware. However, we identified a tendency SMEs to consider HF as a possible strong means to detect and mitigate cyber threats. Therefore they consider it is necessary to pay special attention to the role of the human factor in the field of cybersecurity in Bulgaria. At the same time, we identified as the key problem the level of competencies and the insufficient capacity (knowledge and skills) of IT staff. Therefore, the SMEs consider as an important mitigation strategy improvement of recruitment, education, training, and retention of IT personnel, as well as the process of lessons learned from cybersecurity practice. The data shows that despite the recognised importance of HF in cybersecurity, the training still is not sufficient.

We believe that the results of the SMEs survey will be a valuable instrument for the public administration of the Republic of Bulgaria in their work to improve the process of institutional capacity building to tackle cyber threats, as well as in recruitment, E&T and retention of cyber warriors.

Acknowledgement

This paper presents part of a conducted research for strengthening the administration of the subject "Cybersecurity and opportunities for application of innovative technologies in the work of the state administration in Bulgaria," supported by The Bulgarian Institute of Public Administration (IPA).

References

1. Brian M. Bowen, Ramaswamy Devarajan, and Salvatore Stolfo, "Measuring the Human Factor of Cyber Security," *2011 IEEE International Conference on Technologies for Homeland Security* (HST), Waltham, MA, 2011, pp. 230-235, https://doi.org/10.1109/THS.2011.6107876.
2. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, (Brussels: European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, 2013).
3. Chris Forsythe, Austin Silva, Susan Stevens-Adams, and Jeffrey Bradshaw, "Human Dimensions in Cyber Operations Research and Development Priorities," in *Foundations of Augmented Cognition*, edited by Dylan D. Schmorrow and Cali M. and Fidopiastis (Berlin, Heidelberg: Springer Verlag, 2013), 418-422.
4. Fredrik Karlsson, Joachim Åström, and Martin Karlsson, "Information Security Culture – State-of-the-art Review between 2000 and 2013," *Information & Computer Security* 23, no. 3 (2015): 246-285, https://doi.org/10.1108/ICS-05-2014-0033.
5. John S. Leggitt, Olga G. Shechter, and E. Lang, *Cyberculture and Personnel Security: Report I – Orientation, Concerns, and Needs* (Monterey, CA: Defense Personnel Security Research Center, 2011).
6. NATO, *Defending the Networks: The NATO Policy on Cyber Defence. NATO Policy on Cyber Defence*, endorsed by Allied Defence Ministers in June 2014.
7. *Human Systems Integration Approach to Cyber Security*, STO Technical report TR-HFM-259 (Paris: STO, 2020)
8. Marcus Nohlberg, "Why Humans are the Weakest Link," in *Source Title: Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, edited by Manish Gupta and Raj Sharman (Hershey, PA: Information Science Reference-IGI Global, 2009), 15-26.
9. Angela Sasse, Sasha Brostoff, and D. Weirich, "Transforming the 'Weakest Link' — A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* 19, no. 3 (2001): 122-131, https://doi.org/10.1023/A:1011902718709.
10. Carsten Winkelholz, S. Traber, F. Kruger, H. Gunther, F. Flemisch, C. Semling, N. Wlczek, and H. Schaub, *Human Factors for Cyber Defence. Human Systems Integration for Resilient, Cooperatively Automated Cyber Defence Systems* (Brussels: European Defence Agency, 2014).

About the Authors

Captain (BGR-N) (ret.) Yantsislav **Yanakiev** – see p. 6 of the the editorial article in this volume, https://doi.org/10.11610/isij.4400.

Assoc. Prof. Dimitrina **Polimirova**, Ph.D. received her M.Sc. degree of Economics at New Bulgarian University. In 2008 she received her Ph.D. at National Laboratory of Computer Virology at Bulgarian Academy of Sciences, where she has been working since 1999 and specializes in computer virology. Her research activity is related to the analysis and risk assessment of the information security of file objects exposed to information attacks. As a specialist and researcher, her activities are related to the research and classification of new computer viruses as well as evaluation of a given class of viruses. Her main activity in the last years is in providing of consultancy and expertise in the field of computer, communication and information security and the restoration of application or system data of corporate and consumer configurations of government and state institutions, business organizations and end-users. Since 2013 she has been a Director of the National Laboratory of Computer Virology – BAS. She has participated in the building of various programming and information products serving scientific and state institutions and business organizations. Member of the Advisory Scientific Council at the Managing Board of the Bulgarian Academy of Sciences "Information and Communication Sciences and Technologies." She is co-editor of one book, author and co-author of more than 30 articles in journals or conference proceedings; member of the Union of the Bulgarian Mathematicians. *E-mail*: dimitrina.polimirova@nlcv.bas.bg