Information & Security

V. Shalamanov, V. Sabinski, T. Georgiev
vol. 46, no. 1 (2020): 13-26
https://doi.org/10.11610/isij.4601

Published since 1998

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

Research Article

# Optimization of the Chief Information Officer Function in Large Organizations

*Velizar Shalamanov* [a] (✉), *Vassil Sabinski* [b], *Trayan Georgiev* [c]

[a] *Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, Bulgaria, http://www.iict.bas.bg/EN*

[b] *European Union Military Staff, CIS Directorate, https://eeas.europa.eu/headquarters/headquarters-homepage/5436/european-union-military-staff-eums_en*

[c] *Ministry of Defence, Sofia, Bulgaria, https://www.mod.bg/en/*

ABSTRACT:

The analysis of the process of establishing Chief Information Officer Function in the Bulgarian Ministry of Defence in 2000 and in North Atlantic Treaty Organization in 2020 is used to identify the critical elements for success of the change management process and full realization of the strategic benefits for the organization. Differentiation between the governance of IT and management of capabilities and services for the federation of business organizations is considered as a framework to develop and optimize the CIO function in relation to service provision. The approach proposed in this article combines the COBIT framework with the Analytic Hierarchy Process method for decision making and architectural design and business process optimization to provide a sound basis for consensus in the development of the CIO function. The approach is tested in instituting the CIO function in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences (a federation of more than 40 entities) and its implementation for national and EU level is then defined as a roadmap. Core elements of the approach are tested in the framework of the ECHO project under H2020 for development of a governance model of the European cyber security collaborative trusted network organization.

ARTICLE INFO:

RECEIVED: 03 MAY 2020
REVISED: 31 AUG 2020
ONLINE: 15 SEP 2020

KEYWORDS:

CIO, Governance, Management, IT capabilities, IT services, Collaborative Network Organizations, Optimization, ECHO project



✉ E-mail: shalamanov@acad.bg

## Introduction

### *CIO Function Optimization*

Development of Chief Information Officer function comes with the understanding the value of Information and communication technology (ICT) for the organization on strategic, executive level. Other driver, related to this is the amount of money spent on ICT. Third dimension is the criticality of ICT – availability of information and protection of information. The situation changes dramatically nowadays with the digitalization endeavour going on everywhere around. Last, but not least, the requirements for a New Way of Working, now extended to a New Way of Living with the COVID crisis, will drive our move to the cyber space, where as a comparison with the physical space we have the CIO as a Chief / Great Architect of the Universe.

So there are at least two approaches - one is the evolutionary approach with growing role of ICT and increased ICT budgets. There is another approach when digitalization is main transformational effort in the reengineering the whole organization.

When it comes to transformation we change processes, organization, technology and people in parallel. It looks like the ICT is the driver, being objective (for the government the technology is external, coming from industry), but in reality what we really change are the processes, organization and retrain / develop people to implement the new processes in a new organization with the changing technologies.

In this paper our focus is on CIO function driving the technology insertion in government organization through managing change for digital transformation with focus on processes, organization and people.

Specific area is cyber resilience and building proper governance and management of collaborative networked organization on National level as well as for European Union (EU) and North Atlantic Treaty Organization (NATO) to support the change management efforts of the government CIOs.

As mentioned, today the organizations are highly dependable on information technology (IT) not only to run their businesses but also to stay competitive. To realize the planned operational or strategic benefits the organization has to rely on CIO. It is observed that the responsibilities of CIOs embrace a wide range of duties, indicating their importance in the organization. The activities of CIO are related to re-engineering the existing business processes and their management, identifying new capability to use the new technologies, planning and integration of physical infrastructure and its accessibility, identifying and exploiting the company's resources, maintaining cyber resilience of the organization, etc.

The CIO is a member of the top C-class management teams that play a critical role in strategy design and therefore greatly affect organization performance due to their role in the decision-making process. The results show that the interaction between Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), Chief Technology Officers (CTOs), and CIOs can improve organization

performance. The role of top management is vital for planning, but CIO should provide motivated alternative decisions to cope with different challenges. Some enthusiastic CIO promotes innovative development methods, new software applications, or the use of new IT devices. The more reasonable way is to form a board of top managers along with the CIO to discuss the challenges and requirements of the strategic IT innovations and to ensure consistently and reliable IT-enabled operations.

Digital transformation requires constant engagements in order to estimate the applicability of new technologies in the context of specific hardware requirements. In this regard, the CIO should be able to react first if these new technologies are applicable to the business need of the organization. If the answer is positive, the required infrastructure is to be evaluated in respect of two possible ways: to upgrade or to be changed with a new (most probably in a waves with managing transition for a period of years). This is not easy task and CIO should be capable to determine the required short-term and long-term changes.

This paper makes a difference between the CIO function and Communication and Information Organization (C&IO) to build and operate cyber space in support to the business organization and following the policy, guidance and requirements as well as the resource constraints defined by the CIO function.

The paper elaborates first the CIO function in a single organization and National level, explores the current developments in NATO and EU (defence dimension) as international organizations.

Next step is a review of the development of CIO function and C&I organization for Bulgaria in the defence sector. Short review of the current effort for the development of a CIO function in academic sector is presented.

The goal is to define the research questions for deeper analysis of the CIO function development in Bulgaria in order to optimize it, based on the experience in other countries, NATO, EU and through piloting / testing it in the Institute of Information and Communication Technologies (IICT).

## CIO in a Single Organization

Information and communications technology is changing the way organizations and individuals operate. The speed and pace of this change is constantly accelerating and the increasing complexity of the networks and systems matches the growing demands we place on them. We expect to share information and data seamlessly across our organizations and beyond and at the same time our increasing reliance on technology leaves us vulnerable to cyber-attacks from a wider range of threat actors than ever before. New technologies present both opportunities and risks to NATO and it is vital that we adopt a coherent, strategic approach to safeguard and enhance our technological and security edge.

The shortage of skilled Chief Information Officers has a major impact on the ability to plan and manage information resources and reengineer processes, the quality of projects being developed and technical specifications, financial

planning and the provision of network and information security. The role of the CIOs is crucial for the success of the public administration.

The CIOs of leading organizations describe a consistent set of six key principles of information management that they believe contribute to the successful execution of their responsibilities, according to a research made by the United States General Accounting Office.[1] These principles touch on specific aspects of their organizational management such as formal and informal relationships among the CIO and others, business practices and processes, and critical CIO functions and leadership activities. The CIOs interviewed considered these principles instrumental because they address critical organizational and operational aspects of the CIOs role.

These six fundamental principles and key characteristics of CIO Management in leading organizations described by the CIOs are:

*Recognize the Role of Information Management in Creating Value*

- Information management organizational functions and processes are incorporated into the overall business process.
- Mechanisms and structures are adopted that facilitate an understanding of information management and its impact on the organizations overall strategic direction.

*Position the CIO for Success*

- The CIO model is consistent with organizational and business needs.
- The roles, responsibilities, and accountabilities of the CIO position are clearly defined.
- The CIO has the right technical and management skills to meet business needs.
- The CIO is a full participant of the executive management team.

*Ensure the Credibility of the CIO Organization*

- The CIO has a legitimate and influential role in leading top managers to apply information management to meet business objectives.
- The CIO has the commitment of line management and its cooperation and trust in carrying out projects and initiatives.
- The CIO accomplishes quick, high-impact, and visible successes in balance with longer term strategies.
- The CIO learns from and partners with successful leaders in the external information management community.

*Measure Success and Demonstrate Results*

- Managers engage both their internal and external partners and customers when defining measures.

[1] *US GAO, Chief Information Officer, Executive Guide, GAO-01-376G.*

- Management at all levels ensures that technical measures are balanced with business measures.
- Managers continually work at establishing active feedback between performance measures and businesses.

*Organize Information Resources to Meet Business Needs*

- The CIO organization has a clear understanding of its responsibilities in meeting business needs.
- The extent of decentralization of information management resources and decision-making is driven by business needs.
- The structure of the CIO organization is flexible enough to adapt to changing business needs.
- Outsourcing decisions are made based on business requirements and the CIO organizations human capital strategy.
- The CIO organization executes its responsibilities reliably and efficiently.

*Develop Information Management Human Capital*

- The CIO organization identifies the skills necessary to effectively implement information management in line with business needs.
- The CIO organization develops innovative ways to attract and retain talent.
- The CIO organization provides training, tools, and methods that allow skilled IT professionals to use in performing their duties.

## National Approaches

The most well-known example is that of United States, establishing CIO in 1996 under the regulations of the defence Authorization Act.

There are different views how to implement the CIO function, varying country to country and comparative analysis is under way in our IICT team to identify the alternatives, based on clustering of the models used in USA, Canada, UK, Australia, Germany, the Netherlands.

In the United States the CIO (at US national level) and CIO Council is designed to establish standards against which the achievement of all agency programs can be measured. This includes many functions as monitoring the performance of Federal Government programs, optimizing information resources and investments, aligning IT solutions with Federal enterprise business processes, adopting and sharing best practices, attracting and holding qualified ICT workforce, managing risks, ensuring security and so on. The Chief Information Officers Council (CIO Council) is established. The CIO Council ensures the principal interagency coordination.

The path to digitalisation in the Netherlands for example led to the introduction of new job title (Chief Information Officer (CIO)) in the national government with the main focus of ensuring better project management, especially in the field of innovations. The so called Coordinating CIO in Nederland supposed to advise political leadership and high level civil servants on large scale ICT

projects. One of the most important CIO duties is to furnish the Dutch Parliament with complete, timely and accurate information related to the ICT projects and their progress.

In Germany, the Chief Information Officers Council (CIOC) is made up of the CIOs from each German federal ministry, and the Federal IT Management Group. The Commissioner for Information Technology chairs this group and works in close cooperation with them. The CIOC serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The Council's role includes developing recommendations for information technology management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's IT workforce.

This comparative study is in the initial stage, but results will be presented at the DIGILIENCE 2020 to inform the discussion of the development of a CIO function in Bulgaria – 20 years after establishment of the first CIO in MoD in June 2000.

## CIO in a Networked Organization

International organizations are classic example of federated network of bodies that require effective and efficient ICT support. It is very much the case on national level, but well documented experience of the two major organizations, Bulgaria is member of, are very useful for the development of the Bulgarian national model to follow in the next phase of digitalization.

### *The NATO Approach*

On international level most recent effort is taken by NATO in order to strengthen coherence function and achieve a comprehensive approach to use of ICT in support to the Alliance. Below are some key elements of the concept agreed among nations through a yearlong consultation process.

The key challenge for NATO is how to create coherence across the 41 separate NATO civil and military bodies (employing more than 20,000 users) that form the NATO Enterprise. The Consultation, command and control (C3) Board, with national experts, has studied the current situation in detail and their analysis identifies some gaps in Enterprise-wide coordination and integration of large investment programmes with a focus on local rather than Enterprise improvements. There is no single management mechanism for decisions affecting the communications and information systems across the Enterprise. The NATO networks and technical infrastructure becomes more complex, but oversight and management of these systems remains fragmented limiting the opportunity to fully exploit technological benefits and adequately protect information and communication technology. Improved coherence will enable implementation of an effective, fit-for-purpose information and communications technology strategy.

Coherence is to ensure efforts are channelled to holistically address and fulfil NATO's requirements. For NATO, getting coherence right will deliver benefits in terms of improving our capability delivery across the Enterprise, setting the conditions to enable data exploitation, improving cyber defence posture through a reduction of the attack surface and sharper focus on information security. It will provide a centralized function to enable agility in the face of disruptive technology and adaptability to innovative approaches.

NATO currently does not have a function or individual responsible for implementing, monitoring and managing information technology coherence at the Enterprise level. It is expected Nations to establish an Enterprise Coherence Authority, that extends across all the NATO Enterprise bodies.

The post of Director of the CIO Office, known as the NATO CIO, is envisioned to have Enterprise oversight on cyber issues to enable cyber awareness, and in close coordination with all relevant NATO civil and military bodies to work towards the continual improvement of the NATO Enterprise cyber hygiene and cyber defence posture. The NATO CIO could be responsible for the development of Enterprise directives and advice on the acquisition and use of information technologies and services considering the implications of independent initiatives on the Enterprise. Key responsibilities could be expected to be:

1. Communications and Information Vision Implementation;
2. Alignment to NATO's Goals and Objectives;
3. Senior advisor to decision makers, including Enterprise Requirements;
4. CIO Programme of Work;
5. Compliance;
6. Information Technology watch;
7. Communications and Information Systems Operational Authority.

The NATO CIO interacts with the C3 Board, the Military Committee (MC), the Agency Supervisory Board (ASB) of the NATO Communications and Information Organisation and provides support to the Cyber Defence Committee and Security Committee.

The Senior Executive Group (SEG) could comprise of the NATO CIO, senior staff from the International Staff, International Military Staff, the Strategic Commands, NATO Communications and Information Agency and NATO Support and Procurement Agency, with representation decided by the heads of the respective NATO Enterprise bodies (potentially CIOs of these bodies). The group is to coordinate and discuss C3 capabilities, Information and Communications Technology services and other information technology matters affecting the Enterprise. The responsibilities of the Group could be for coordination of Enterprise directives and advice, developed by the CIO Office, on information and knowledge management, the acquisition and use of information technology capabilities and services, and to consider implications of independent initiatives on the Enterprise. This group is key to coordination across the Enterprise.

The CIO office is to have an integrated staff composed of members of the International Staff and International Military Staff. The Office is to support the Senior Executive Group agendas, prepare record and monitor progress of action items and their advices.

The Implementation Plan is under development. The plan acknowledges the significant change programme the introduction of a CIO function across NATO will entail and the significant resource implications noted by the Resource Planning and Policy Board. Phase 1 starts with the establishment of the CIO project office tasked with delivering the Initial Operating Capability (IOC) of the NATO CIO function. Each annual report will constitute an intermediate decision point, allowing for steering a flexible resourcing schema (with gradually adjusted resources to discharging responsibilities, based on the CIO advice, including through drawing resources from NATO Enterprise entities) which could lead to a revision of the start date of Phase 2. At the end of Phase 1, an informed decision could be taken on whether or not to resource a permanently established function (Phase 2), based on a review of the benefits achieved and informed by advice from the Military Committee, Resource Policy and Planning Board (RPPB) and C3 Board.

### *CIO Function in the EU*

In EU there is Directorate-General for Communications Networks, Content and Technology (DG CONNECT) dealing with digitalization in the European Council (EC) and in the EU Military Staff (EUMS) there is CIS/Cyber division for planning and management of ICT support for the military activities. The Union has specialized Agencies as European Engineering Learning Innovation and Science Alliance (ELISA), European Union Agency for Cybersecurity (ENISA) and others dealing with CIS/Cyber issues on execution level and under new regulation is envisioned to develop an European Cyber security Centre of Competence with a network of National Cyber Coordination centres to facilitate the development of an European Cyber Security Community and improve the competence and competitiveness of the EU entities in Cyber domain.

So, within the EU institutions, there is no single body or office dealing with CIO functions and responsibilities, neither in the civilian/political domain nor in the military domain.

In the European Commission, there are two main structures:

- Directorate-General for Informatics (DIGIT) with a mission to deliver digital services to enable EU policies and to support the Commission's internal administration. DIGIT has the responsibility to provide the Commission, and whenever appropriate other European institutions and bodies, with high quality and innovative

- Workplace solutions: creating new ways of working and collaboration for staff;

- Business solutions: delivering information systems supporting rationalised business processes within the framework of the corporate IT governance strategy;
- Infrastructure solutions: providing reliable, cost-effective and secure infrastructure and services;
- Effective solutions: aligning IT investments with business priorities, facilitating relationships with our strategic partners, balancing risk with business value for the Institution;
- Support the modernisation of public administrations by promoting and facilitating interoperability so that European public administrations can work seamlessly together across boundaries – Interoperability solutions.

DIGIT's vision is to take on and drive forward the digital leadership role within the Commission. DIGIT must develop and lead the digital transformation of the Institution so that it can deliver EU policy better, more efficiently and more productively, fully seizing the opportunities offered by new technologies.

- Directorate-General for Communications Networks, Content and Technology (DG CONNECT) conceives and implements the policies required to create a digital single market for more growth and jobs, where citizens, businesses, and public administrations can seamlessly and fairly access and provide digital goods, content and services.

DG CONNECT fosters a modern, secure, open, and pluralistic society and help drive the digital transformation of European industry and public services using innovative digital technology and support for the development of digital skills. They are developing a long-term vision using the potential technology breakthroughs and flagships, to improve peoples' lives and to increase the competitiveness of the European economy at large and its key sectors. In addition, the Union has specialized Agencies as ENISA and others dealing with CIS and Cyber issues on execution level. Under the new Regulation, it is envisioned to be established European Cyber security Centre of Competence with a network of National Cyber Coordination centres to facilitate the development of European Cyber Security Community and improve the competence and competitiveness of the EU entities in Cyber domain.

In the European External Action Service (EEAS), there are two organizational structures dealing with CIS and Cyber functions:

BA.BS.3 (Information Technology Division) defines the Information and Communication Technology (ICT) strategy and delivers ICT services to support EEAS objectives and activities, both in EEAS Headquarters and in Delegations. The scope of BA.BS.3 activities is limited to Unclassified and EU Restricted information. The CIS&CD Directorate promotes the EUMS' / Military Planning and Conducting Capability's (MPCC) interests during the most relevant ICT governance processes, in order to ensure that the provided ICT systems / services meet the military specific operational requirements of the two EEAS bodies with key roles on EU Common Security and Defence Policy (CSDP) arena. Having regarded the

MPCC's role as the military strategic command of the EU non-executive missions, and the associated need for a dedicated robust, reliable and secure Command and control (C2) information system, the access of EU Training Missions (EUTMs) to the EU Restricted environment provided by EEAS is currently under discussion / analysis during the CIS&CDD - BA.BS.3 - MPCC CJ6 coordination efforts.

BA.SI.3 (Secure Communications Division) is responsible for the protection and registration of European Union Classified Information (EUCI) within all EEAS entities and during the transfer to Member States, other EU institutions, International Organisations, agencies and missions by the provision of classified communication and information systems (CCIS), along with the infrastructure, organisation, personnel and information resources required to develop, maintain and operate them. Within this role, BA.SI.3 is the main provider of secure ICT systems / services for the EU CSDP military user community, with focus on EUMS, MPCC and their connections to MoDs/EU MSs, EUTMs, EU OHQs/FHQs, other EU Agencies, as derived from the information exchange requirements.

For the development of the military policies and guidance for implementation, operation and maintenance of CIS and Cyber Defence in support of CSDP activities the responsibility lays with the CIS&CD Directorate (CIS&CDD) within the EU Military staff.

The CIS&CDD provides expertise and/or personnel to strategic and operational advance and real-time planning for military CSDP operations, missions, exercises and trainings and provides guidance for the development of EU military policy, concepts, requirements and guidance for CIS and Cyber Defence in support of military/civilian CSDP activities. CIS&CDD contributes to EUMS planning through the provision of CIS&CD planning expertise at the strategic and operational level, and provides the CIS element of crisis response planning and assessment for operations and exercises.

In the light of the need to act innovatively, and based on the positive experience of some EU MS with the establishment of a National Defence CIO, the CIS&CD Director at his last conference at the end of 2019, recommended to respective directors of EU MS to start an open-ended discussion on the introduction of an "EU Defence CIO". Along with the recent developments to strengthen EUs capabilities to perform Command & Control over non-executive and executive military CSDP missions and operations, the need for interoperability and alignment of military C2 capabilities encompassing all phases of an operation/mission from planning to execution became eminent. A strong advocate for in-time development, effective management, delivery and operation of resilient, reliable and secure military capabilities are of utmost importance for the success of our operations. This applies likewise to the cooperation with MSs, partners and EEAS internally. Some EU MS have already acknowledged this need and have taken actions to establish this role within their respective organisations. While NATO is on its way to investigate the benefits of such a function, within the EU the discussion has only commenced within the military domain.

Transparent discussion of this important topic with adequate consideration of all available options is overdue.

The detailed study of the consolidation of the CIO function in EC and EU MS is under way and results will be presented at the DIGILIENCE 2020 conference in Varna.

### *CIO and C&I Organization – the NATO Example*

NATO C&I organization (NCIO) was established as of 1 July 2012, based on the Summit 2010 decision of the NATO HoSG. Core of the NCIO is NATO C&I Agency with its Agency Supervisory Board (ASB) to provide organizational governance in partnership with other bodies exercising governance authority as C3 Board, Cyber Defence Committee (CDC), NATO Security Committee (NSC), and Resource Policy and Planning Board (RPPB) under overall authority of North Atlantic Council (NAC).

The organization includes all Multinational programs and C&I Partnerships established by the ASB as part of the Organization.

CIO function, as described above is under discussion and it includes NATO coherence authority vested in the Secretary General, NATO CIO, supported by the CIO Office and Senior Executive Group, formed in principle by the CIOs of the NATO bodies.

This construct is quite complex and comprehensive and is in the process of continuous improvement through the consultations among 30 Nations, so could be considered as a universal model to provide good practices of developing national C&I organizations and CIO function and vice versa – to be developed itself, based on best national practices.

Currently under development is the second edition of a Strategic Direction and Guidance for the NCIA that obviously should be based on an updated NCIO Vision 2025+. The development of this vision is influenced by policy and operational developments in NATO as well as the reflection process for the improved consultations and decision-making process in NATO to be supported by the NCIO. Establishment of the NATO wide coherence role in C&I domain as well the position of NATO CIO, together with the improvement of the customer funding regulatory framework in C&I domain are driving changes in the area.

The authors are considering a study on NATO developments in order to draft good practices for national implementation at least for Bulgaria.

### *CIO and C&I Organization in the Ministry of Defence of Bulgaria for the last 20 years*

In 1999 at the end of the 20th century Bulgarian MoD invited US DoD to perform a joint C4 Study in order to develop a plan for improved interoperability, security and overall modernization of the C4ISR systems of the defence establishment of Bulgaria. With a strong support from USEUCOM and MITRE, the study was accomplished in 2000, and based on the recommendation the function of CIO was established with a regulation for the life cycle support of the C4ISR

systems and recommendations were approved for the long-term development of the communication and information (C&I) systems in accordance with the Military Doctrine of 1999.

In addition of the CIO function vested in the J6 Directorate with the support of the C4ISR program Committee and respective bodies represented there, the step was taken to establish a solid C&I organization under the Minister – Strategic CIS as a service provider and capability developer for the main C&I services of the defence establishment (going beyond MoD).

Study of this experience of more than 20 years of development of the CIO function is under way to be presented at the CIO function optimization round table, planned in parallel of the DIGILIENCE 2020 conference.

### *CIO Function Development in IICT-BAS and the Academy at large*

In 2010 in the Bulgarian Academy of Sciences several ICT related institutes were consolidated in a National ICT institute to cover all areas of knowledge required for successful digital transformation and cyber resilience, to include areas of traditional strength in the BAS as HPC and AI / NLP, robotics / embedded intelligent systems, GRID and other ICT network s, and others.

In 2019 with the approval of the strategy for the development of the IICT till 2030 the focus was given to digital transformation and cyber resilience for effective, efficient and secure use of ICT. As result of this the institute established formal CIO/CISO/DPO functions for improvement of the e-Infrastructure and its security and at the same time to consolidate the research in ICT Governance and management, Cyber Resilience and decision-making support for CIO role, establishing of ICT Academy, based on an e-Platform for multi-stakeholder approach to development of advanced digital competencies and skills.

Study of the initial 2 years of implementing of the IICT Strategy in the area of CIO/CISO/DPO and ICTA is underway to be presented at Digilience 2020 to inform further development and contribute to the final report of the established by the Chair of the Academy Consultative Council on effective efficient and cyber resilient management of ICT resources in BAS – scheduled for the end of 2020.

## Conclusion: CIO Competencies, Career Development and Certification

All above mentioned studies are oriented to identify the key competencies and to define a career development model for the CIO/CISO/DPO personnel in Academy of Sciences, but Public administration as well. These studies are building upon joint work with the SA e-Government and the Institute of Public Administration (IPA) in 2017-2018 to develop IT Leadership Academy and accomplish a study on improvement of cyber security in PA with implementation of new IT as AI and blockchain.

Results of the studies – on national and BAS level, using the experience of other countries and organizations as NATO and EU is oriented to the development of a national certification for CIO/CISO/DPO program in contribution to the national endeavour in the area of digitalization and cyber resilience. Such a

certification program will be proposed as part of the National Research Program ICT in Science, Education and Security – in particular Task 3.2.1.

## Acknowledgement

The preparation of this paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICT in SES)," financed by the Ministry of Education and Science of the Republic of Bulgaria.

## References

1 Velizar Shalamanov and Todor Tagarev, *Information Aspects of Security* (Sofia: Procon, 1996). – in Bulgarian.

2 C4 Study, US DoD – MoD-Bulgaria, 2000.

3 *Lifecycle Management of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4I) systems in the Ministry of Defense and the Bulgarian Armed Forces* (Sofia, Military Publishing House, 2000).

4 Anthony Gerth and Joe Peppard, "The Dynamics of CIO Derailment: How CIOs Come Undone and How to Avoid," *Business Horizons* 59, no. 1 (2016): 61–70.

5 Janis Gogan, Kieran Conboy, and Joseph Weiss, "Dangerous Champions of IT Innovation," in *53rd Hawaii International Conference on System Sciences, Maui, Hawaii 2020*, pp. 6144–6153.

6 Dilian Korsemov, Daniela Borissova, and Ivan Mustakerov, "Group Decision Making for Selection of Supplier under Public Procurement," *ICT Innovations 2018. Engineering and Life Sciences*, edited by Slobodan Kalajdziski and Nevena Ackovska (Cham: Springer, 2018), 51-50, https://doi.org/10.1007/978-3-030-00825-3_5.

7 Velizar Shalamanov, "Institution Building for IT Governance and Management," *Information & Security: An International Journal* 38 (2017): 13–34.

8 Daniela Borissova, Zornitsa Dimitrova, and Vasil Dimitrov, "How to Support Teams to be Remote and Productive: Group Decision-Making for Distance Collaboration Software Tools," *Information & Security: An International Journal* 46, no. 1 (2020): 36-52.

9 Velizar Shalamanov, Vladimir Monov, Gergana Vassileva, Ivo Blagoev, Silvia Matern, and Ivan Blagoev, "A Model of ICT Competence Development for Digital Transformation," *Information & Security: An International Journal* 46, no. 3 (2020), https:/doi.org/10.11610/isij.4619.

10 Mitko Stoykov, *Integrated System for Command and Control in Extraordinary Situations: Architecture* (Sofia, Softtrade, 2006).

11 Ivan Sariev, *Information Management* (Sofia, Classics and Style, 2007).

12 Velizar Shalamanov, Georgi Penchev, Silvia Matern, "Digitalization and Cyber Resilience Model for the Bulgarian Academy of Sciences," *Proceedings of DIGILIENCE 2019, Studies in Systems, Decision and Control* (Springer Nature Switzerland AG, 2020), in press.

[13] Corien Prins, Dennis Broeders, Henk Griffioen, Anne-Greet Keizer, and Esther Keymolen, *iGovernment* (Amsterdam: Amsterdam University Press, 2011).

[14] CIO.gov, https://www.cio.gov, last accessed September 2020.

[15] IT Law Wiki, https://itlaw.wikia.org, last accessed September 2020.

[16] NATO, www.nato.int, last accessed September 2020.

## About the Authors

Dr. Velizar **Shalamanov** is Deputy Director of the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences, Associate Professor in its "IT for Security" department, and Chairman of the Agency Supervisory Board of NATO C&I Agency. After 19 years in the military, followed by an academic career in the Academy of Sciences, he served in several leadership position, including as deputy minister of defence (1998- 2001) and minister of defence (2014) of Bulgaria, and Director Demand Management in the NATO's Communication and Information Agency (2009-2017). Currently he is focusing on consolidation of the academic cyber capacity in Bulgaria and research in a H2020 research project. In parallel, he is engaged in non-governmental and political activities aiming to better position Bulgaria in NATO and the European defence. https://orcid.org/0000-0001-9388-7293

Brigadier General Vasil **Sabinski** is Director CIS, EU Military Staff European External Action Service since August 2017. He holds a master's degree in Telecommunications from the "Vasil Levski" National Military University. He has broad experience in the field of CIS in the Bulgarian Armed Forces at different levels. In 2010, he was selected to be the Branch Chief for CIS Policy and Requirements within the EU Military Staff in Brussels, a position he held for four years before going back to Bulgaria to become the Commander of the Stationary CIS of the Bulgarian Ministry of Defence and Armed Forces. Promoted to General rank in August 2017, he returned to the EU Military Staff to assume the position of Director CIS with responsibility for developing policies and guidance for CIS and cyber defence in support of the EU Common Security and Defence Policy operations and missions.

Trayan **Georgiev** holds a M.Sc. degree as engineer of Computing equipment and Automated Systems for control of troops (ASCT) from Higher Military School of Artillery and Air Defence "Panayot Volov," Shumen, Bulgaria (1997) and an MBA degree from the New Bulgarian University in Sofia (2014). He is a graduate from the US Army Command and General Staff College, Fort Leavenworth, Kansas, USA (2008). He has extensive international experience in SEEBRIG, NATO International Military Staff and Bulgarian Delegation to NATO. Currently, he holds the rank of Lieutenant Colonel and works as Chief expert at the Defence Policy and Planning Directorate in the Ministry of Defence, Bulgaria. LTC Georgiev works in the areas of defence policy and planning, consultation, command and control (C3) and cyber defence.
https://orcid.org/0000-0002-6213-4501