Information & Security: An International Journal

Velizar Shalamanov, vol.38, 2017, 5-10 https://doi.org/10.11610/isij.3800

TOWARDS EFFECTIVE AND EFFICIENT IT ORGANIZATIONS WITH ENHANCED CYBER RESILIENCE

Velizar SHALAMANOV

This volume of *Information and Security: An International Journal* aims to establish a baseline for a multiyear study on IT governance and management of large national and international IT organizations aiming to increase effectiveness, efficiency and cyber resilience – their own and of the customers they serve. The objectives are to identify best practices, develop a maturity model and processes for assessment, compliance, change management and continuous improvement.

Modern society and organizations are highly dependent on information technologies. At the same time, rapid changes in technology, vulnerabilities of cyber domain for attacks, interoperability challenges, increased cost of the IT systems, critical shortage of specialists and many other factors call for improved governance and management of IT. In response, the collection, analysis and managed use of good practices form the approach, largely implemented nowadays.

We consider NATO as an excellent laboratory for identification of best practices in many areas, including IT governance and management, for effective, efficient and cyber resilient IT organizations, due to the very nature of the Alliance. NATO provides well developed consultations and decision making system, a very demanding customer base and availability of a sufficiently large budget; it also has an executive agency to address the customer requirements in most effective and efficient ways, where cyber security is the ultimate priority.

At the Lisbon Summit of 2010, heads of states and governments of NATO nations decided to consolidate all IT organizations of NATO in one service-based and customer-funded agency, as shared IT service centre capable to support not only common funded NATO structures, but any other eligible customers – national or multinational. This transformation effort challenged all 28 (now 29) nations and agency team to work together in identifying the best governance and management practices for increased effectiveness and efficiency in IT support with visible savings in com-

parison to the situation in 2010 and, at the same time, to consider cyber defence as essential part of this activity.

Further improvement of IT governance and management at national and international level will depend on our ability to identify, learn and implement lessons, and to turn them into an actionable set of best practices. This initiative includes, but is not limited to the topics below, with the aim to contribute to the improvement of IT governance, management and cyber resilience, especially in the security sector, but also in other public organizations. The experience of NATO Communications and Information Organization (NCIO) is of special interest as it is based on intensive and constructive consultations among 28+ nations and many organizations in the evolution of a very complex IT organization – the NATO Communications and Information Agency (NCIA).

Understanding the need for recommendations that are truly actionable and applicable, the I&S Editorial Board announced a call for papers with the aim to take a snapshot of current status of good practices with related practical examples, coming from national or international environment, covering:

- Institutionalization of IT governance and management
- Stakeholder management for complex IT organization
- Role of Chief Customer Officer in IT organization
- Strategy development for complex IT organization
- Internal audit missions for effective change management
- Risk management in complex IT organization
- The utility of dashboards as governance mechanisms
- Architectural approach in IT management
- Customer funding models for IT organizations
- Innovation management in IT organization
- Outsourcing and acquisition in large IT organization
- Service catalogues and service level agreements
- Governance and management of IT capability development
- Personnel management in complex IT organizations.

As a first step, this 2017 volume presents original papers that cover key aspects of the experience in NATO (NC3A/NCIA) and Bulgaria (relatively new NATO and EU member on the South-East border of the alliances) with focus on institution building, customer funding and acquisition, and key elements of cyber resilience (including research and technology development challenges).

In 2016, through a joint declaration NATO and EU identified cyber defence as a key area of cooperation. Digital endeavours of NATO are supported by NCIA. EU is driving digital transformation with the strong digital agenda of member nations, working individually and in collaboration to identify and implement best practices in this journey to the future through many different IT organizations. As every transformation, this one will change processes, organizations, technologies and people to achieve new levels of effectiveness and efficiency with a high degree of resilience to cyber attacks.

The European Union, being part of the West around NATO, is the most diverse and dynamic environment of many nations, but our hypothesis is that when it comes to IT organizations' effectiveness, efficiency and cyber resilience, the roots are in the best NATO practices of digital transformation around the development of NCIA as the IT organization of the Alliance. Hence, in our study we plan to use the NATO approach as a point of reference.

Authors of the seven papers in this volume come from two main strands. Five of the authors have an extensive experience in the development of NC3A/NCIA as the NATO IT organization, while the other four combine research with considerable practical engagement in improving IT organizations in Bulgaria and the EU. This already serves as an excellent bridge between the practitioners and the research communities.

The volume is structured along three themes. The first two articles address general issues of governing IT organizations. First, the editor of this volume presents a general framework for governance and management of a large international IT organization as a reference of identified lessons and good practices to be used in further studies of effectiveness, efficiency and cyber resilience of IT organizations.[1] The article is based on the practical experience of the author in the period 2012-2016 as part of the change management team to consolidate, rationalize and optimize the operation of five separate IT organizations merged into one – a period in which the author served as director demand management in NC3A for NATO and Nations and in NCIA covering the full spectrum of customers for the largest NATO agency. The second article addresses stakeholder engagement as a key element of the governance to provide effective decision making and support for the operation of the IT organization .[2] It reflects the experience of the author as a Chief Strategy Officer of NC3A, later of NCIA.

Customer funding and acquisition in an IT organization is the theme of the second block, including three articles. First, the architect of the model of customer funding for NC3A—the first NATO agency using this regime—identifies and describes a lot the key lessons from the implementation of this approach.[3] Then, an experienced

team member of the Chief Operating Officer (COO) group elaborates on the challenge a non-for-profit, customer funded agency faces in balancing demand and capacity to break even.[4] The article draws valuable lessons of interest to many public IT organizations and their customers. The block is closed by a contribution from an acquisition officer (deputy direcor of acquisition in NCIA) and reflects her experience of more than decade both in NC3A and NCIA in dealing with procurement of products and services using various vehicles, including Basic Ordering Agreement (BOA).[5] It clearly relates to requirements of defence organizations for quality and speed, and in particular the support to operations by meeting urgent requirements.

The third block addresses the development of capacity for cybersecurity and resilience. The first contribution describes practical experience of using Computer Assisted Exercises (CAX) to strengthen the cyber resilience of various administrative organizations, building on previous work in the field of crisis / emergency management exercises.[6] The final article in this volume presents an architecture developed by the authors to manage research activities in support of cyber security and resilience.[7] In addition to the already standard ICT and cyber-physical systems strands of research, the architecture covers studies of UxVs, bio-integrated systems and cognitive processes, all treated in an integrated manner in a systems of systems framework.

In the future, we intend to seek input from other international IT organizations, e.g. directorates in European Commission, the EU agency for large information systems (eLISA), the CIS division of EU Military Staff, the European agency for network and information security – ENISA (and the future EU Cyber Agency), the EU Joint Research Centre, as well as national IT organizations, contributing to the digital transformation in the NATO-EU space, in order to identify best practices for the evolving maturity models and compliance assessment – recognized essentials for effectiveness, efficiency and cyber resilience requirements. This is an academic effort to consolidate the knowledge towards a general theory of IT organizations, understanding that nowadays, with the digital transformation, ever more organizations are de facto becoming most of all IT organizations.

We believe that with this first I&S volume on best practices in IT governance and management, and each of the high quality contributions to it, there will be better understanding of the framework and approach to the enhanced effectiveness, efficiency and cyber resilience of large IT organizations – both national and international. The topic is certainly not exhausted; our intention is to solicit more contributions towards the development of a maturity model and compliance process and to define the scope of a project on improvement of cyber resilience of IT systems through effective and efficient IT governance and management using, *inter alia*, best NATO practices. The process will be facilitated by establishing partnerships with NCIA, the Emerging Se-

curity Challenges division of the NATO International Staff and other in order to combine efforts to:

1. Collect and analyse best practices to build the body of knowledge;
2. Develop a maturity model for cyber resilience;
3. Develop change management model for strengthening cyber resilience;
4. Assess the maturity level of key IT organizations;
5. Develop change management plan for assessed IT organizations;
6. Organize IT leaders training and certification;
7. Institutionalize a Centre for Effectiveness, Efficiency in IT governance and management for cyber resilience.

A side effect of this study is the development of the course for IT leaders (CIOs) on information resource management and cyber resilience, included in the catalogue of the Institute of Public Administration of the Bulgarian Government for 2018. We consider the study as a contribution to the initiative on digital transformation of the public administration, started by seven European universities with a CIO course in Thessaloniki in October 2017.[8]

References

[1] Velizar Shalamanov, "Institution building for IT Governance and Management," *Information & Security: An International Journal* 38 (2017): 13-34, https://doi.org/10.11610/isij.3801.

[2] Paul Alan Smith, "Stakeholder Engagement Framework," *Information & Security: An International Journal* 38 (2017): 35-45, https://doi.org/10.11610/isij.3802.

[3] Paul Ballinger, "Lessons from a Customer-Funding Regime in a Large IT Organization," *Information & Security: An International Journal* 38 (2017): 49-62, https://doi.org/10.11610/isij.3803.

[4] Jean-René Couture, "Reconciling Operational and Financial Planning Views in a Customer-Funded Organization: Making Customer-Funding Work for NC3A," *Information & Security: An International Journal* 38 (2017): 63-69, https://doi.org/10.11610/isij.3804.

[5] Agata Szydelko, "Acquisition in a Large IT Organization," *Information & Security: An International Journal* 38 (2017): 71-76, https://doi.org/10.11610/isij.3805.

[6] Irena Nikolova, "Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector," *Information & Security: An International Journal* 38 (2017): 79-92, https://doi.org/10.11610/isij.3806.

[7] Todor Tagarev, George Sharkov, and Nikolai Stoianov, "Cyber Security and Resilience of Modern Societies: A Research Management Architecture," *Information & Security: An International Journal* 38 (2017): 93-108, https://doi.org/10.11610/isij.3807.

[8] Managing the Public Sector Digital Transformation: A Training Course for Public Sector CIOs and IT Leaders. Thessaloniki: International Hellenic University, available at http://web.ihu.edu.gr/mdt2017/.

About the author

For a short CV of Dr. Velizar Shalamanov—Member of the Editorial Board of *Information & Security: An International Journal* and Editor of this volume—see p. 34 of the accompanying article, https://doi.org/10.11610/isij.3801.