Information & Security

Velizar Shalamanov
vol. 42 (2019): 49-66
https://doi.org/10.11610/isij.4203

Published since 1998

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

Research Article

Organising for IT Effectiveness, Efficiency and Cyber Resilience in the Academic Sector: National and Regional Dimensions

Velizar Shalamanov

Institute of Information and Communication Technologies, Sofia, Bulgaria
https://IT4Sec.org; http://www.iict.bas.bg/EN/index.html

ABSTRACT:

This article presents an architecture and analysis of the change management aspects of security in public administration, developed as part of a study of best practices in the management of IT organisations with emphasis on effectiveness, efficiency and cyber resilience. The analysis served as a basis for defining a model of academic support to cyber resilience. The implementation envisions use of the BEST environment (Basic/budget Environment for Simulation and Training), which was initially developed for the crisis management domain and later adapted to support organisational and human risks analysis in the cyber domain in research and training activities on cyber resilience. This environment is used for PESTEL analysis of the cyber environment to identify a model for resilience from organisational and human perspective and to support SWOT assessment of the possible implementation paths in order to select the most suitable among all qualified solutions and provide training of the personnel involved. Regional aspects of cyber resilience are addressed in the context of the NATO/EU framework, limited to the academic area. Finally, the article addresses organisational and human aspects and presents a concept of an Academic CERT Association at national level and the possibilities to use it as a model for a regional network.

ARTICLE INFO:

RECEIVED: 10 Dec 2018
REVISED: 04 Mar 2019
ONLINE: 13 Mar 2019

KEYWORDS:

cyber resilience, network governance, governance model, consolidation, coordination, regional cooperation

E-mail: shalamanov@acad.bg

Digital Transformation

Modern society and organisations 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 with special focus on cyber resilience.[1] In response, the collection, analysis and managed use of good practices form a promising approach, already largely implemented.

This paper has as main focus the public administration (PA). We assume the study is applicable for the security sector, but it is not explicitly covered here. The intention is to cooperate in the future with business / industry entities in their digital transformation (e.g. the transition to Industry 4.0) as well. An ongoing study in the Institute of Information and Communications Technologies (IICT) [2] with partners—primarily the Institute of Public Administration [3] and the State e-Government Agency [4]—to establish a baseline for a multiyear research on IT governance and management of large national and international IT organisations, aiming to increase effectiveness, efficiency and cyber resilience (E2CR) – their own and of the customers they serve is providing initial input for the development academic E2CR organisation.[5] The objectives of the study are to identify best practices, develop a maturity model and processes for assessment, compliance, change management and continuous improvement.

On Figure 1 we consider the following players in digital transformation of the public administration (DTPA): PA itself, an IT organisation tasked to digitise the PA, customers / stakeholders, industry to which the IT organisation outsources (contracts) support for DTPA, academia to provide Research and Development (R&D) and Education and Training (E&T) support to DTPA, international level PA (other nations and international organisations the PA is dealing with).

Our focus is on the academic support to DTPA and particularly on effectiveness, efficiency and cyber resilience of IT organisations of PA (the security sector and industry at large will be covered at a later stage).

This paper defines the scope of the study for the academic support to digital transformation and cyber resilience. The purpose is to develop National Scientific Program in Cyber Resilience (or even E2CR) and to establish a National Coordination Centre in the context of the EU regulation.[6] On the next level, regional cooperation is covered in the framework of NATO, EU and other relevant international organisations and, finally, key elements for research and cooperation are identified, based on the experience in the defence field.

Figure 2 presents the basic architecture for the cyber resilience study in PA. This structure follows the best practices of years of research in security sector governance, based on the understanding, that defining an optimal organisation for cyber security (E2CR) in terms of efforts is similar to that of defining an optimal organisation of the security sector at large. Specific architecture for the study of cyber resilience from technology perspective is based on the initial work of the team to define cyber security research program [7] in Bulgaria. The

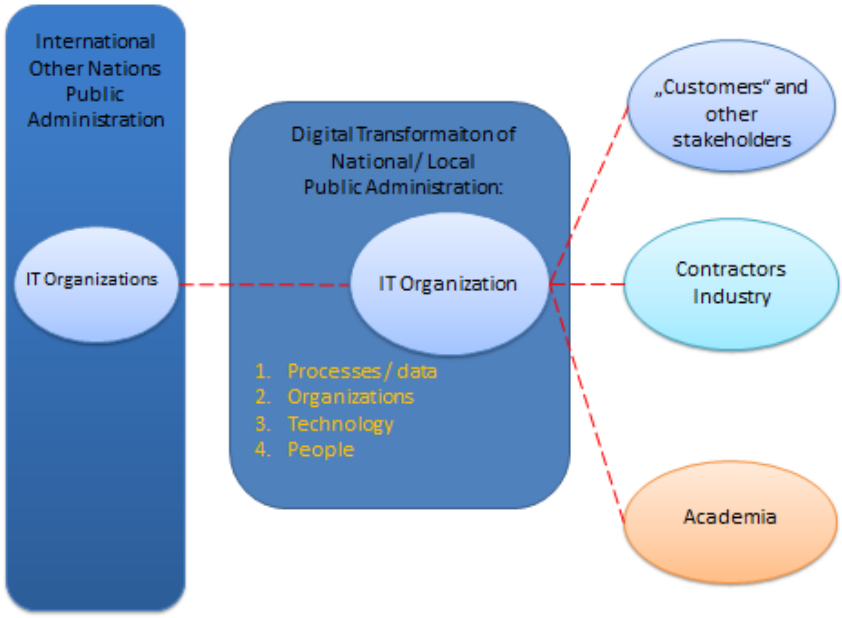

Figure 1: Players in digital transformation of the public administration.

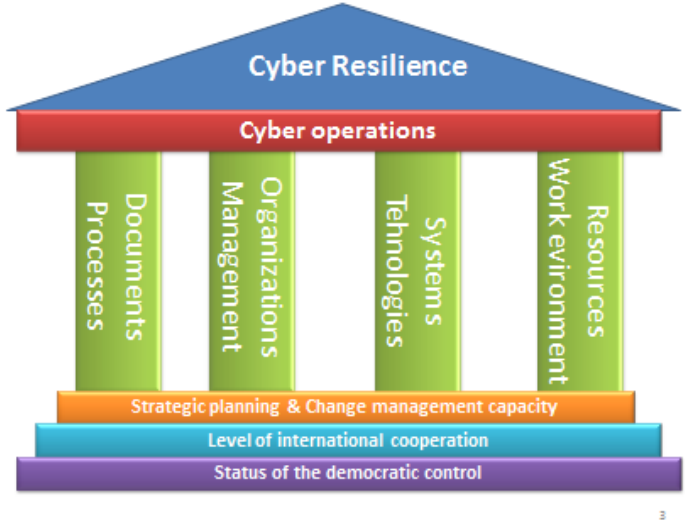

Figure 2: Architecture of the cyber resilient organisation.

study on cyber resilience is informed by the 2016 Cyber Security Strategy of Bulgaria and especially the model for transition from focusing on *cybersecurity* to emphasising *collaborative resiliency*.[8]

Academic Support to Digital Transformation and Cyber Resilience

In order to support the study and future cooperation in implementation of a critical ICT/ cyber projects we initiated the process of consolidation of the expertise in Bulgaria in a form of federated network—an *Academic CERT Association (ACERTA)*—where 'CERT' could be red as both Cyber Environment Resilience Team or, in the more traditional understanding, as Computer Emergency Response Team (CERT). This also reflects the historical fact that the first CERT in Europe was established in 1992 by the Dutch Academic provider SURFnet (SURFnet-CERT3). Currently, the European Union agency for cybersecurity ENISA accounts for more than 100 teams around Europe.

ACERTA is covering PESTEL (Political, Economic, Social, Technological, Environmental and Legal) scope of analysis – it means expertise on effective, efficient and cyber resilient ICT organisations in different fields*: policy / political (including governance), economic / resource (incl. management), social, technological, environmental, legal.*

In the IICT, being an academic entity, we focus on R&D and E&T, not so much on operational issues, but of course with a readiness to be mobilised in support of operational CERT/CIRC when and as required. The model of E-GOVLAB[9] in Sweden is envisioned as useful to develop the ACERTA federation in support to public institutions and industry.

Following the best practices of organisational design for the development of ACERTA as an academic pillar of cyber resilience system we consider the following founding elements for Mission, Vision, Strategy and Implementation plan. The development of ACERTA is in the context of a synchronised spiral in the four dimensions of the digital transformation (Figure 3).

Mission: Consolidate the expertise for comprehensive academic support to development of effective, efficient and cyber resilient (E2CR) IT organisations in Bulgaria and the region, following and contributing to the best practices in the NATO/EU community.

Vision: Federated academic environment to include established research and training/ consultation processes with matrix organisation and supported by connected labs, using collaboration/ innovation technology as a platform for knowledge development and engaging large group of people, representing all the stakeholders of digital transformation. The next level will be a customer funded, service-based network of expertise to support cyber innovation for effective, efficient and resilient cyber domain.

Strategy:

1. Start small, but think global – NATO/EU environment with regional implications.
2. Keep it as an academic endeavour and grow evolutionary in this environment.

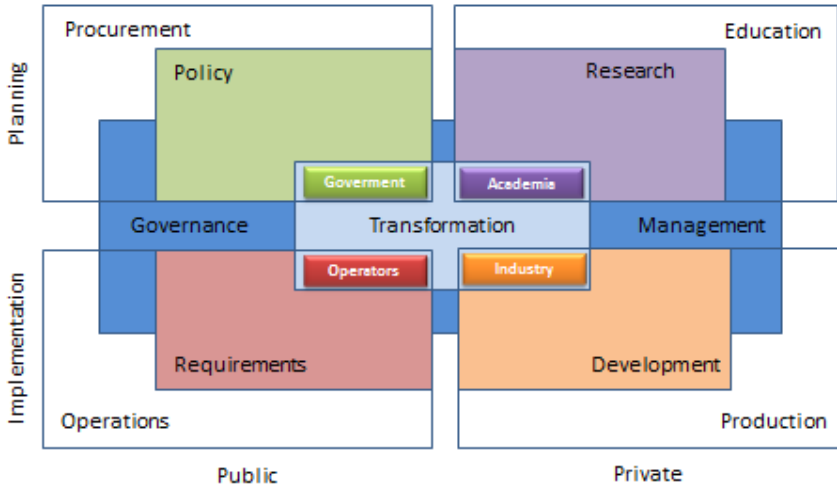

Figure 3: Dimensions of digital transformation.

3. Engage and effectively communicate with other stakeholder communities – Government, operators, industry in Bulgaria.
4. Seek partnership with NATO/EU bodies in the area, on bilateral level with similar organisations in leading countries and in the region.
5. Special focus on non-for-profit cooperation with NCIA and active participation in IST panel of STO.
6. Establish a Steering Board and an annual or multiyear Program of Work (PoW) for ACERTA on national level.
7. Seek networking for projects under EU Framework programmes (e.g. Horizon 2020) for research and position ACERTA as a National Coordination Centre (NCC) under the EU regulation for the establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

Implementation plan:

Year 1:

a. Agree on mission, vision and strategy;
b. Consolidate the expertise in the Institute of Information and Communication Technologies, the Bulgarian Defence Institute, and the European Software Institute – Centre Eastern Europe (ESI-CEE) in an initial

Academic CERT Association with a distributed laboratory environment;

c. Consolidate the Internet presence and develop "Information & Security: An International Journal" as a platform for E2CR of IT organisations study of best practices and their implementation;
d. Engage IPA and the "G.S. Rakovski" Defence and Staff College to establish a certification program for Chief Information Officers (CIO) for the public administration.

Year 2:

a. Extend to other units of the Bulgarian Academy of Sciences and academic elements of the ministries of defence and the interior, dealing with E2CR of IT organisations;
b. Define the Value proposition and a business model;
c. Engage customers and all types of stakeholders;
d. Organise a National CIO conference, coordinated with EU and NATO CIO annual conferences.

Year 3:

a. Develop a catalogue of academic services to support E2CR of IT organisations;
b. Register ACERTA as an academic pillar of the Cyber Reserve and NCC;
c. Engage universities to adapt IT Governance and Management courses, Cyber Resilience courses to the best practices studied in ACERTA;
d. Organise Regional ACERTA meeting and establish Balkans / Black Sea ACERTA in NATO/EU framework.

It is essential to start with the academic IT infrastructure (e-Infrastructure) – the acad.bg domain (connecting the bas.bg domain and other academic networks with associated research labs) in order to test good practices in a limited environment and build upon this experience to develop maturity models and selection of best practices to be used in other domains. Under the European GRID initiative there is an opportunity to explore international model of sharing resources and providing services, seeking effectiveness, efficiency and cyber resilience.

The process will be facilitated by establishing partnerships with NCIA, the "Emerging Security Challenges" division of the NATO International Staff and respective EU bodies, CIO institutions / academic elements in EU/NATO nations 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 organisations;
5. Develop change management plan for assessed IT organisations;

6. Organise IT leaders training and certification;
7. Institutionalise an organisation for Effectiveness, Efficiency in IT governance and management for cyber resilience in the Bulgarian Academy of Sciences.

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 [10] 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.[11]

Consolidating national academic expertise in ICT/Cyber area, our goal is to provide support to Bulgarian public administration and security sector in the process of digital transformation and at the same time to form a partnership with similar entities from EU nations in order to participate in Horizon 2020 (and future framework programs) as well as in the European Defence Industrial Development Program, while on the NATO side to seek partnership for Smart Defence Cyber projects and Science for Peace and Security (SPS) funded projects with partners in the Western Balkans and the Black Sea Region.

Organisational Aspects and External Relations

With an agreement on a key processes and initial capabilities to be developed and maintained, this section addresses the organisation of the ACERTA. An optional organisation as a network of academic bodies is presented on Figure 4. It is based on voluntary commitment of academic / NGO structures to provide experts in the expert pool and to select representative roles (legal identity, CEO) as well as a coordinator (kind of Chief Operations Officer, or COO) of different projects to be run by the experts of the ACERTA – either internal or external under contract signed by the Representative of ACERTA.

In this a way ACERTA will be capable to run the National Scientific Program on Cyber Resilience and to play a role of NCC under the EU regulation, when approved by the Parliament.

BEST – Cyber (Basic Environment for Simulation and Training) is an environment based on a federation of capabilities (labs) of different participants. As experts, people from bodies not members of ACERTA could be invited. Some of the teams could be working as a service provision team instead of a project team.

Projects / services could be just consulting or training activities, but could be R&D, experimentation, demonstration and other academic activities in support of external customers, including in programs as Horizon 2020, European defence industrial development programme (EDIDP) and others.

Based on the initial study of the profiles (competences) of the academic organisations, the current experiment for ACERTA is based on the membership of:

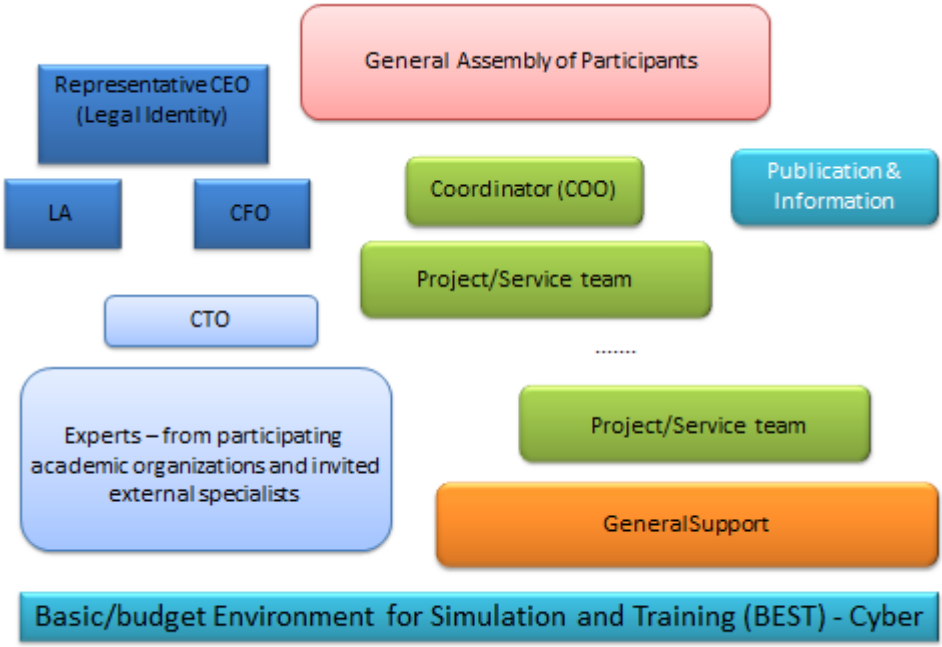

Figure 4: Organisation of ACERTA.

a. Institute of Information and Communications technologies from the Bulgarian Academy of Sciences / IICT-BAS (with main contribution from the "IT for Security" department);
b. Defence Institute "Prof. Tsvetan Lazarov" of the Ministry of Defence (with main contribution from the C4ISR directorate);
c. European Software Institute – Central and Eastern Europe / ESI-CEE (with main contribution from the Cyber Lab located in the Sofia Tech Park).

This is related to the Bulgarian academic participation in ECHO consortium (**E**uropean network of **C**ybersecurity centres and competence **H**ub for innovation and **O**perations) created in response to the Horizon 2020 call for "Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap" (SU-ICT-03-2018).

The key roles in ACERTA are:

1. Representative (CEO – Chief Executive Officer);
2. Coordinator (COO – Chief Operating Officer);
3. Senior Research Fellow Economic aspects (CFO – Chief Financial Officer and economics advisor, acquisition / public procurement support);

4. Senior Research Fellow Technology (CTO – Chief Technology Officer);
5. Senior Research Fellow Research Infrastructure / BEST-Cyber (CIO – Chief Information Officer);
6. Senior Research Fellow Policy (POLAD – policy adviser, publications & information);
7. Senior Research Fellow Social aspects (SCO - StratComms officer);
8. Senior Research Fellow Environmental aspects (EA – environment adviser);
9. Senior Research Fellow Legal Affairs (LA – legal adviser).

Profiles (competences) of the key members of ACERTA are defined as follows.

The Representative (CEO) is selected by the General Assembly for three years and the Coordinator for two years in order to maintain the dynamics of the operations. The Coordinator works with experts (organised in groups with senior research fellows on Policy, Economic aspects, Social aspects, Technology, Environmental aspects, Legal issues) to identify and prepare projects and facilitate project implementation in ACERTA through the small project support office (PSO).

Through his/her organisation, the CEO provides the function of CFO [12] and acquisition/ public procurement [13] support for ACERTA. The role of the public relations officer (publication and information / dissemination) could be offered by any of the participating organisations, eventually under POLAD.

The key role of COO [14] is to manage the portfolio of projects, where the team members for projects (SME/Subject Matter Expert resources) are coming from the pool, maintained by the CTO, which provides technical coherency for the projects and oversight on the development of BEST-Cyber.

BEST-Cyber as a distributed experimentation and training support environment is managed by dedicated CIO to manage all information resources of ACERTA. The main functionalities of BEST-Cyber are presented on Figure 5. Special attention is given on the development of Computer Assisted Exercises (CAX) as a service, based on the experience of managing several exercises [15] in the cyber domain recently.

ACERTA's current operations are based on active projects of joining organisations, seeking synergy for their individual success, but more important is the ambition to define a future Program of Work (PoW) and service offer to the customers and partners at National, NATO/EU and regional levels.

ACERTA, as shown on Figure 3, works in partnership with the governments, operators and industry in the field of R&D and education and training (E&T) from academic non-for-profit perspective to support the digital transformation.

Figure 6 presents the added value of ACERTA, being the third dimension in the relations "Government – IT Industry" and "EC/NATO – Government," as well as "EC – IT Industry." In addition, ACERTA, with the support of EC/NATO, Government and IT Industry could transfer good practices from Western Europe to

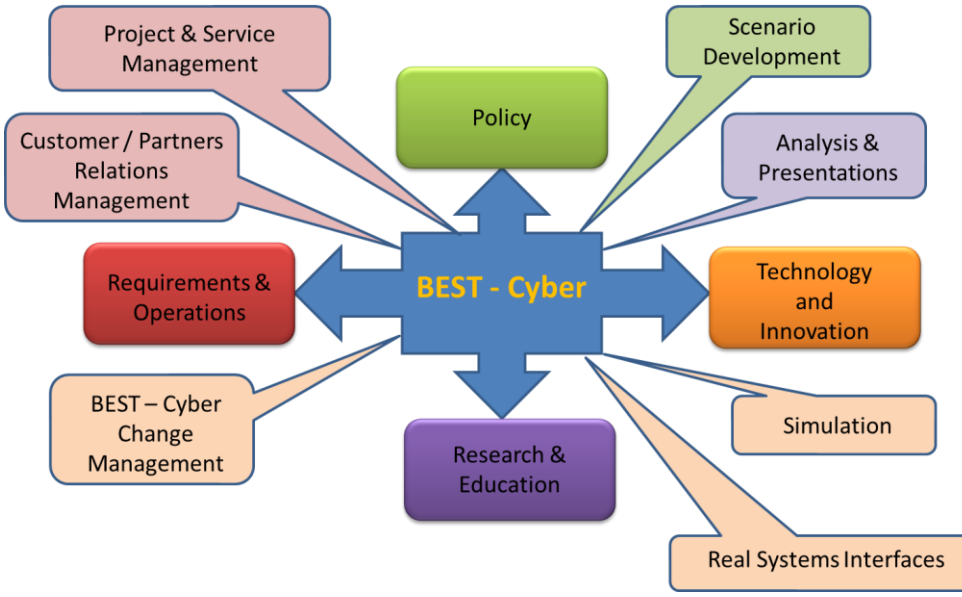

Figure 5: Functionality of the BEST-Cyber as experimentation and CAX environment.

the countries in the Western Balkans and the Black Sea region (i.e. in the Eastern Partnership of the European Union).

In addition to ACERTA, a critical element is the Innovation Centre, based on membership from Government and Industry to provide pre-competitive services, using the contribution from the Government, Industry and Academia as well as the European Commission and NATO in order to prepare the ground for effective competition for solutions provided by the Industry to the Government and the European Commission and NATO.

Regional Cooperation in Digital Transformation – Academic Aspects

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 the NATO Information and Communication Agency (NCIA). The European Union 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 organisations. As every transformation, this one will change processes, organisations, technologies and people to achieve new levels of effectiveness and efficiency with a high degree of resilience to cyberattacks.

The European Union, being part of the West around NATO, is the most diverse and dynamic environment for many nations. Yet, the author shares the hypothesis that when it comes to IT organisations' effectiveness, efficiency and

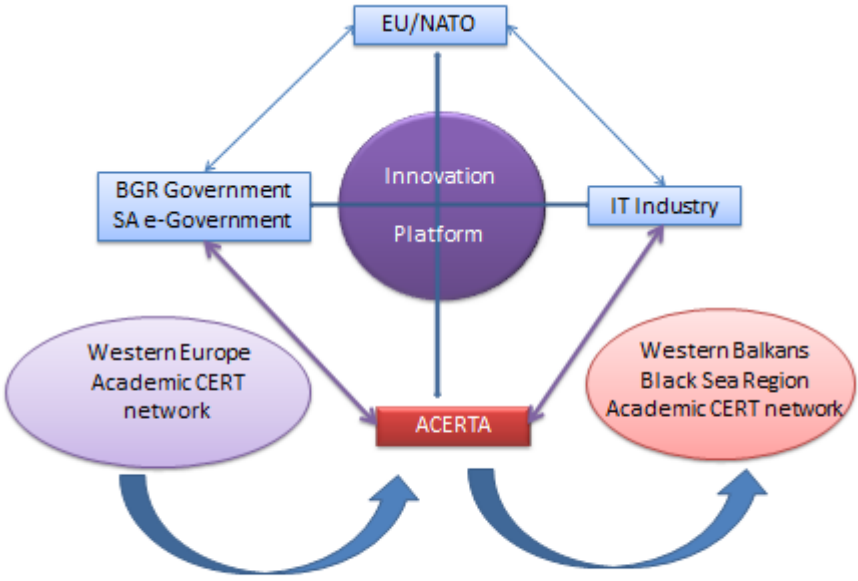

Figure 6: The role of ACERTA for improvement of Government – Industry relations in the framework of NATO/EU developments.

cyber resilience, the roots are in the best NATO practices of digital transformation around the development of NCIA as the IT organisation of the Alliance. Hence, in our study we plan to use the NATO approach as a point of departure.

In the framework of NATO and the EU we consider the regional cooperation (presented on Figure 7) emphasising that it is seen as extension of the development of ACERTA in Bulgaria to address requirements in the region in a collaborative manner with similar structures of other countries and in the framework of NATO and EU developments. Regional cooperation is shaped by the other international formats of cyber-related activities under UN and OSCE umbrellas as well.

Our focus is on bringing first class expertise and best practices in the area of digital transformation from NATO and the EU to Bulgarian customers in the public administration and the security sector through the mechanisms of the academic R&D and E&T for E2CR of ICT organisations and to seek cooperation with entities dealing with digitalisation of industry under such initiatives of the EU as the “Digital Innovation Hubs.”

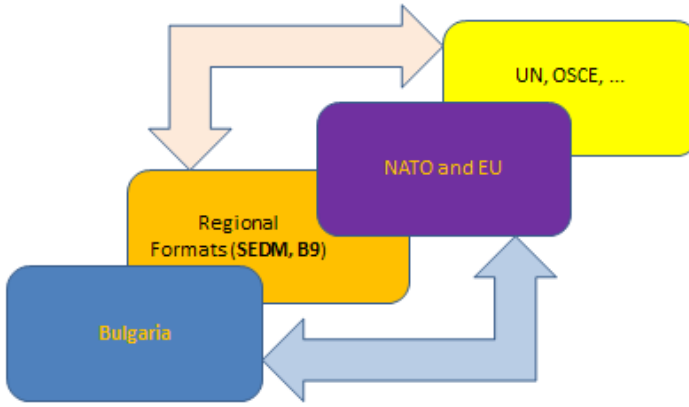

Figure 7: Levels of cooperation with focus on transferring or contributing best practices from/to EU and NATO and the regional role of Bulgaria.

It is recognised that most effective in the cyber resilience context is the regional cooperation – because of distance to travel, culture, shared educational and research programs. In this context, for Bulgaria there are at least three regional formats to explore – South-Eastern Europe [16] (to include integration of Western Balkans to EU and NATO), the Black Sea Region (with Moldova, Ukraine, and Georgia as a priority partners at NATO/EU context) and the most homogeneous format of Bucharest 9 (B9) initiative (all the countries from Estonia to Bulgaria – former Warsaw pact members and now members of NATO and the EU).

In all these formats critical are the level of national consolidation of the expertise, the capacity for and the maturity of its governance and management, and the relations with the Government, operators and industry. For this reason, before moving to extended regional cooperation it is necessary to assess the national level of maturity, possibly through an academic CERT study based on self-assessment and comparative analysis with a predefined model of good practices and conditions for an effective regional cooperation.

The alignment of academic structures will have a very positive effect on the harmonisation of the development in other quadrants of digital transformation – government, operators and industry. Based on our experience, it is most cost effective to achieve a good level of regional cooperation in the academic area using national, NATO (including the Science for Peace and Security programme) and EU programmes (Horizon 2020 and other). Established federation in aca-

demic environment is a tool afterwards to develop a strategy and a plan for alignment in other dimensions of digital transformation and especially in the field of cyber resilience.

This means that we need to define the regional approach as a scope – geographical and functional, develop self-assessment project and agree on a maturity model, based on a set of good practices to be implemented at every level. Implementing self-assessment could give us enough information for a regional conference on defining minimum cyber resilience requirements for the region in order to achieve Cyber Resilience Situational Awareness (CRSA) capability and define a model for the National Cyber Security Centres (NCSC), federated on regional level and capable to share information with EU and NATO bodies in the cyber domain.

Key Elements for Research and Cooperation

On national, regional and EU/NATO level we need a typical transformation programme, inspired by the overall process of digitalisation. Cooperation takes place on several levels – alignment of Cyber resilience strategies and processes, development of a framework for organisational development and technologies to be used, harmonised approaches for human factor development in the cyber domain. Initial research on resilience of the academic e-Infrastructure was initiated by the Ministry of Science and Education of Bulgaria in the 2018 National ICT Research Program. In parallel, IICT works with regional partners (Croatia, North Macedonia) on very practical level for the creation of a network of academic centres for improvement in regional context of two main capabilities, currently under development for defence domain, but with high value for academic and government e-Infrastructure:

- Cyber Resilience Situational Awareness (CRSA); and
- National Cyber Security Operations Centres (NCSOC).

The objectives of the CRSA area are:

- Implement the selected CRSA solution into the existing NCSOC to provide cyber situational awareness (SA);
- Create an integrated environment whereby data from existing cyber monitoring tools can be fused into the CRSA solution to deliver visualisation of the interdependency between government (incl. information) services and operational missions of critical infrastructures (CI);
- Provide informed decision making, regarding the impact of cyber threats, vulnerabilities and/or incidents on operational missions and services so that rapid remediation action are taken to protect CI;
- Identify and assess what the impact of a cyber-attack, threat and or vulnerability may have upon CI and its mission integrity;
- Provide a common architecture to enable the interoperability and sharing of cyber SA information within the region and with other allies;

- Maximise the government's existing investment in its cyber resilience architecture and associated monitoring tools.

At present, Bulgaria lacks an integrated cyber situational awareness solution (CRSA) – cyber defence tools, such as Security Incident and Event Management Systems (SIEMS) and Vulnerability scanners, generate 'stove piped' information, which is then viewed and reported independently without required integration of cyber information for situational awareness. The CRSA solution should be technologically agnostic and able to utilise a range of data connectors allowing it to ingest data from existing cyber monitoring tools using a range of data transfer formats. CRSA is expected to operate using Virtual Machine (VM) technology and so no additional hardware to be used. The ability to fuse cyber data into one accessible source will allow for its representation using geo-locational dashboards which, when combined with alerts, automated courses of action and consistent remediation processes will allow for:

1. Near real time visualisation of a cyber threat, vulnerability and or incident against key IT assets and the subsequent impact analysis upon operational missions and public administration services;
2. The setting of thresholds, alerts and weightings within the system to protect key IT assets and services;
3. Generation of automated alerts to initiate response, using consistent processes and courses of action (CoA);
4. Improve cyber reaction decision cycle times.

In addition, the CRSA will be the focus for enhancing cyber defence interoperability across the region, NATO and the EU. The establishment of a common CRSA architecture will facilitate the sharing of cyber situational awareness information between allies and partners in the region – similar to exchange for the purposes of air defence. Thereby, having the potential to create an Alliance/region wide cyber situational awareness picture based upon a common architecture will help ensure that there is a consistent level of cyber security situational visibility against a common threat.

The objectives in the establishment of National Cyber Security Operations Centres (NCSOC) and sectoral cyber SOCs are to:

- implement a Security Information and Event Management (SIEM) system to monitor and provide threat intelligence on the e-Infrastructure;
- implement an Intrusion Prevention system to provide network security to the e-Infrastructure;
- provide cyber security of key web applications and services.

These objectives will require research and cooperation on practical implementation of:

- *Security Information and Event Management* solution to provide a robust and layered defence posture against both known, new and emerging network threats. The SIEM correlates 'seemingly unrelated' events and data

from network devices using advanced and sophisticated real-time correlation techniques, including machine learning and artificial intelligence.

- *Intrusion Prevention Systems* with Advanced Threat Appliance (ATA) to detect and counter targeted attacks, advanced threats, and advanced persistent threats (APT) that could penetrate traditional network security solutions by using evasive techniques like slow detonating malware, compromised mobile devices, and hidden payloads. Such a system needs to provide increased protection against APTs with static and dynamic detection techniques using Next Generation Firewall (NGFW) and Next Generation Intrusion Prevention Systems (NGIPS). The use of Threat Digital Vaccine (ThreatDV) service to deliver an enhanced cyber capability to the Bulgarian organisations for protecting its critical information infrastructure.
- *Web Inspect tool* for web application security testing substitution. The Web Inspect tool is a web application security assessment solution designed to thoroughly analyse complex web applications and web services for security vulnerabilities. It quickly identifies exploitable security vulnerabilities in web applications through the complete life cycle from development through production and delivers broad technological coverage, fast scanning capabilities, extensive vulnerability knowledge and accurate web application scanning results.

The implementation of these critical capabilities with the support of the Academic CERT Regional Association to include required R&D and especially education and training, providing expertise for amending the capacity of public organisations with experienced academic staff when required is of critical importance for the improvement of cyber resilience and providing additional positive influence of the resilience of other critical infrastructures on national and regional level. In the last several years, under NATO's Science for Peace and Security programme and with the efforts of George C. Marshall European Center for Security studies in Garmisch-Partenkirchen there is a good regional cooperation on academic level in the cyber domain,[17] that could be exploited in the development of the network of centres of competence in cyber resilience.

Conclusion: A Roadmap to Success

The implementation of any grand Vision starts with the first small steps to bring success and build a fundament for change. In our case, this is the agreement between IICT (the largest ICT academic institute in the country), the MoD's Defence Institute (most advanced public sector institute, working closely with EU and NATO in the area of security and defence), and ESI-CEE (hosting the Cyber Laboratory of the Sofia Tech Park) to start the academic consolidation, using the flexible model of ACERTA as described above.

The second step is to associate ACERTA with an Innovation Centre,[18] being its academic base and contributing to the development of effective relations with

the Government, the European Commission and NATO, and industry on a project or service basis.

The third move is towards a real consolidation along the vision and strategy with focus on building capacity and defining a clear value proposition of ACERTA.

This will lead us to full operational capability with project implementation and service provision for R&D, E&T (including under Exercise / CAX as a service model), based on the BEST-Cyber, attracting representatives from the Government and Industry through the Innovation Centre as a partnership platform.

The regionalisation of this effort is possible in the different formats – South Eastern Europe and it defence ministerial format (for the Balkans and the Black Sea region) and the Bucharest 9 initiative as well with maintaining this cooperation in relevant NATO and EU frameworks. Correlation with other regions – Western Europe (BENELUX, NORDIC Cooperation) is important for European harmonisation of the developments. In this context, the relations with Defence Innovation Greenhouse [19] in the Netherlands and different cyber innovation hubs are to be maintained properly from the very beginning of ACERTA implementation.

These steps will be creating a real ecosystem for innovation through partnership (possibly based on membership fee or other contributions) in R&D, E&T for the pre-competitive / post-competitive (non-competitive) phases of the change management process of digital transformation.

A similar model [20] was tested already in the period 1999-2009 in the area of emergency management and now is time to move the next level in the context of new EU, NATO and National R&D / E&T and public procurement programmes for digital transformation.

References

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

2 Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, http://www.iict.bas.bg/en/.

3 The Bulgarian Institute of Public Administration (IPA), http://ipa.government.bg/en.

4 State e-Government Agency, https://e-gov.bg/wps/portal/agency-en/home.

5 As a first step the President of the Bulgarian Academy of Sciences established in 2018 a Consultative council on E2CR management of information resources.

6 "Proposal for a Regulation of the European Parliament and of the Council on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres," COM(2018) 630 final, 2018/0328 (COD), Brussels, 12 September 2018, https://ec.europa.eu/

commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf.

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.

8 George Sharkov, "From Cybersecurity to Collaborative Resiliency," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense SafeConfig'16*, October 2016, https://doi.org/10.1145/2994475.2994484.

9 eGovLab, https://egovlab.eu/index.php/en/.

10 *IPA Catalogue*, pp. 77-80: http://www.ipa.government.bg/sites/default/files/katalog2018_19_01_2018_4.pdf.

11 "Managing the Public Sector Digital Transformation: A Training Course for Public Sector CIOs and IT Leaders," Thessaloniki: International Hellenic University, 2017, http://web.ihu.edu.gr/mdt2017/.

12 Paul Ballinger, "Lessons from a Customer-Funding Regime in a Large IT Organization," *Information & Security: An International Journal* 38 (2017): 49-62.

13 Agata Szydelko, "Acquisition in a Large IT Organization," *Information & Security: An International Journal* 38 (2017): 71-76.

14 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.

15 Irena Nikolova, "Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector," *Information & Security: An International Journal* 38 (2017): 79-92.

16 Natalia Bekiarova and Marin Petkov, "Opportunities for Development of Defense Cooperation between Southeastern European Countries," *Journal of Innovations and Sustainability* 4 (2018): 39-51.

17 Zlatogor Minchev and Mitko Bogdanoski, eds., *Countering Terrorist Activities in Cyberspace*, NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Vol. 139 (Amsterdam: IOS Press, 2018).

18 InnoCenter Bulgaria, https://en.innocenter.bg/.

19 The Defence Innovation Greenhouse, http://defenceinnovation.eu/.

20 Velizar Shalamanov, "Security Research and Change Management in the Security Sector (The Bulgarian Example in the Period 1999-2008)," in *Change Management Series,* Institute for Parallel Processing and George C. Marshall Association – Bulgaria (Sofia: Demetra Ltd, 2008). – in Bulgarian.

About the Author

Dr. Velizar **Shalamanov** is Deputy Director of the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences and Associate Professor in its "IT for Security" department. 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