Information & Security: An International Journal

Irena Nikolova, vol.38, 2017, 79-92 https://doi.org/10.11610/isij.3806

BEST PRACTICE FOR CYBERSECURITY CAPACITY BUILDING IN BULGARIA'S PUBLIC SECTOR

Irena NIKOLOVA

Abstract: This paper summarizes six years of experience (2011-2016) at the Ministry of Transport, Information Technology and Communications and the National Revenue Agency to develop capacity and cybersecurity readiness. It is based on a number of projects, which adopt a consistent approach for change management and restructuring in public administration in view of cyber security standards. In addition, this paper outlines how digital technologies and simulation tools have been employed in the process of cyber security deployment and capacity development as an example of good practices in the public sector transformation. Using Computer assisted exercises, a special technical platform, training and exercise management system provides an integrated framework across the Public Sector for enhancing the effectiveness and achieving interoperability and analytical capability.

Keywords: Cybersecurity, computer-assisted exercises, simulation tools, public sector.

Introduction

With the digitalization of services and the growing role of technologies, cyber security is becoming more and more important. Cyberspace and its infrastructure are vulnerable to a wide range of risks with both physical and cyber nature/hazards. Skilled cyber actors exploit vulnerabilities to steal information and are developing capabilities to disrupt, destroy, or threaten the delivery of main services.

The most common cybersecurity threats for the government agencies are theft of sensitive information, cyber vandalism, phishing, POS (Proof-of-Stake) and DDoS (Distributed Denial-of-Service) attacks. Today, governments need to be able to handle it and reduce vulnerabilities and damages in complex cyber incidents. They also need to be able to seize the opportunities of the digital transformation, to have the ability to quickly choose between the different alternatives available, often with insufficient information. Competent administration underlies an effective government. Building cybersecurity capacity covers the fundamental concepts underlying the construction of secure systems, from hardware and software to the human-computer interface, with the use of cryptography to secure interactions. These concepts are applied using contemporary trainings, with scenarios drawn from evolving practice, and augmented with hands-on exercises involving relevant tools and techniques.

Applying the modelling and simulation methodologies and tools in the trainings is a new method for capabilities development. In recent years, the Computer Assisted eXercises (CAX) have been used as a powerful approach for the preparation of all-levels authorities in cyber security management, for verification of the level of readiness of the responsible individuals in the organizations and the level of capabilities for mitigating the risks of cyber incidents occurring.

The CAX becomes one of the most effective methods for education and training, which allows to achieve high level of capability at lower prices and decreased risks. The experimentations in the cybersecurity domain in real operational environment can lead to considerable losses for the organizations.

The preparation and implementation of a CAX in the thematic area "Information Security" differs from the typically conducted computer assisted exercises mainly in the scenarios, the modelling and simulation software used for network communications, devices, servers and applications, for the target group of the players – system administrators, information security specialists and to a certain extent, the evaluation criteria.

There has been an exponential growth in the number of cyber security exercises over the past decade globally. This pattern is illustrated in Fig.1.

The number of exercises conducted in Europe in the field of cybersecurity was responsible for over 40% of all global exercises (fig.2).

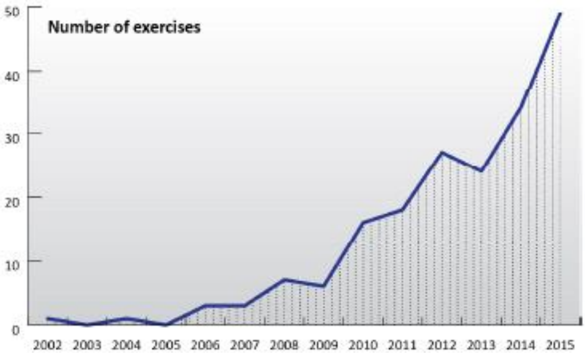

Figure 1: Number of exercises between the years 2002-2015.[1]

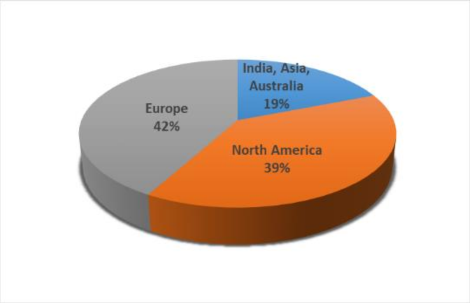

Figure 2: Exercises held in Europe Number of exercises between the years 2002-2015.[2]

The trend is to increase the number of exercises in the coming years. Most important is that the exercises are not only one – time exercises, but also regular recurring initiatives in the form of annual series. That makes it very logical to develop these exercises as a service for better management and lowering the cost.

Cyber security Computer Assisted Exercise

In its nature CAX is a "synthetic" exercise, where the forces and resources are generated, operated and managed in simulation environment.[3]

The Computer Assisted Exercise is an effective tool for individual and collective training for the achievement of a certain level of knowledge for an efficient response in case of information security breaches. The CAX reduces the risk level, enables time jumps and repeated scenarios for a short time interval, as well as simulation of scenarios whose practical implementation is very difficult with unexpected negative consequences. CAX are specifically applicable in situations related to cyber security management, because "recreation" of similar situations in a real environment is too complex, economically ineffective and sometimes unfeasible.

The preparation and execution of CAX in cybersecurity differs from other domain specific computer assisted exercises for crises management, disaster response, military operations etc., mainly in the scenarios, software tools used for modelling and simulation of network communications, devices emulation, virtualization of servers and applications and the targeted training audience.

The realization of a cyber security CAX from the management point of view is a complex activity, which requires specific efforts in the area of the planning and management. Typically, there are three main phases in exercises: planning, execution and evaluation.[4] Adding a structured framework for project management enables monitoring and control on finances, tasks, resources, information, quality, risks and guarantees successful accomplishment of the CAX. In this regard, the Exercise should be planned and executed according to the Project Management Approach – as a specific organization dedicated to deliver its specific results/objectives. In order to achieve required objectives the managers of the project need to have an appropriate toolkit comprising management techniques for planning, executing, assessing and controlling of the project activities. The achievement of the objectives of the CAX project is ensured by good project management, which defines the exercise goals, organises the work packages and assigns the workload to highly motivated, qualified and experienced teams. The applied methodology follows the five phases of the project management lifecycle: initiation, planning, execution, control and monitoring, and evaluation/ finalization. The selection of adequate tools for operating in the management environment depends on the CAX scale, specificity and resources.[5]

The CAX management model is developed at a high level of abstraction, so that it can be interpreted by organizations of various types, structures, sizes, and domains.

This model and respective approach/tools were tested during EU TACOM SEE 2006[6][7] and Phoenix 2010.[8]

The above presented approach for managing the life cycle of a computer assisted exercise in cybersecurity has been used in three major exercises:

- "CYBERWINTER 2011" – first ever for the Bulgarian government administration computer assisted exercise in cybersecurity that was held in the Ministry of Transport, Information Technologies and Communications (MTITC);
- "CYBERNRA 2014" – the first information security computer assisted exercise for the Bulgarian National Revenue Agency;
- "MTCybEx 2016" – Operation level CAX in MTITC using a specialized technology platform – CEP EXONAUT Suite.[9]

Conducting a cyber security CAX in any organization usually aims to validate the specific measures that should be undertaken or procedures that have to be followed during or after an information security incident.

The main goals of a Cyber CAX could be summarized as follows:

- Develop capabilities;
- Evaluate skills/capabilities of individuals, organizations and systems;
- Measure knowledge, ability, endurance, and/or capacity;
- Train the participants and provide an opportunity to gain knowledge, understanding and skills.

The advantages of cyber security CAX find expression in the experimentation and validation of strategies, concepts, policies and procedures (even technologies) for information security before their practical implementation.

CAX players are various depending on the type of the exercise, ranging from expert levels (system administrators, information security officers, experts and administration staff) to managing levels (head of department, director, CEO etc.).

Cyber CAX projects in Public Sector in Bulgaria

CYBERWINTER 2011
Ministry of Transport, Information Technology and Communications

The first CAX for the Bulgarian government administration in thematic area "Cyber Security" was in December 7, 2011 and was held in the MTITC.[10] "CYBERWINTER 2011" was intended to test some specific measures or processes in the event of an information security incident. These measures included cooperation and coordination between the organizational units, as well as the detection of some important interdependencies that cannot be learned in standard training.

In the "CYBERWINTER 2011" took part IT representatives from MTITC and the following executive agencies:

- Executive Agency "Electronic Communication Networks and Information Systems";
- Executive Agency "Automobile Administration";
- Executive Agency "Railway Administration";
- Directorate General "Civil Aviation Administration";
- Executive Agency "Maritime Administration";
- Executive Agency "Study and Maintenance of the Danube River" – Ruse;
- CERT-Bulgaria – National Computer Security Incidents Response Team.

The main project objectives were:

- Enhancing responsible persons capabilities in MTITC, its Agencies and the CERT, to protect the national information infrastructure against cyber-threats and breaches/breakthroughs into information security;
- Identification of organizational and technical vulnerabilities in the information security management system, cybersecurity response procedures and policies;
- Analysing and forecasting the modern threats to the information infrastructure in the Ministry and its Executive agencies.

Following the best practices, for the purpose of the CAX, all participants were put in an 'isolated' environment, located on a common area, separated into the centres according to the operative architecture of the exercise (Fig. 3). A real and simulated environment of participants, infrastructure and software products have been designed and developed for a virtual simulation.

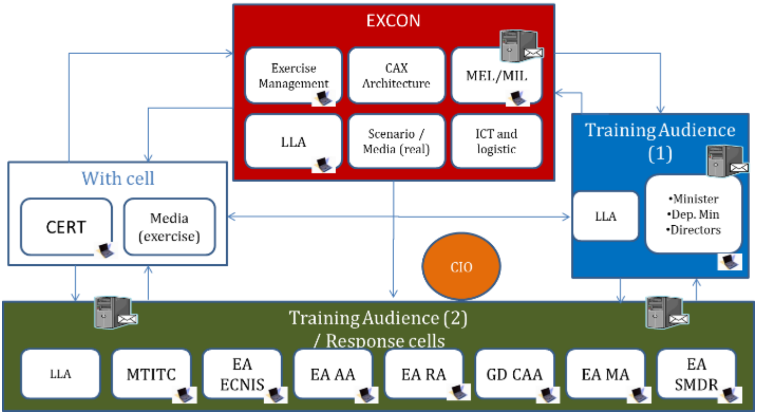

Figure 3: CAX Operational Architecture.

Every participant also played a role, depending on relevant information access. The key scenarios incidents were visualized using software products for modelling and simulating networks, hardware and basic software applications, that helped decision-makers. Each action and response of the players was recorded for analysis of best practices and exercise library.

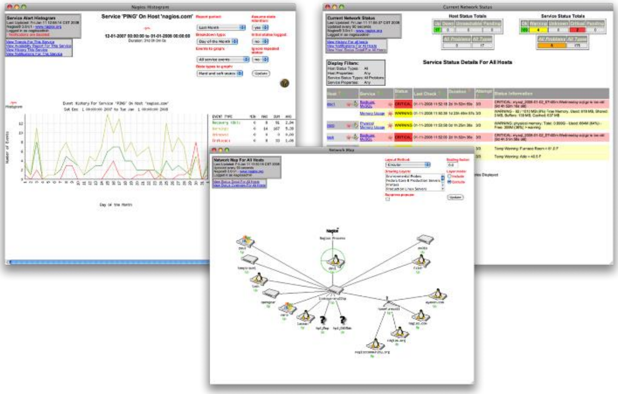

Figure 4: Infrastructure monitoring.

All information during the exercise was available through a system for common operational picture, monitoring the infrastructure (Fig. 4). This information was archived for the purpose of lessons learned analyses.

CAX results

Generally, every cyber security exercise is a success in itself because all participants learn something new and opportunities open up for both their development and the improvement of their organization in the field of information security.

Additional goals and activities verified during the exercise were:

- Response reaction and recovery time;
- Decision-making processes;
- Information sharing (inside and outside the organization);
- Collaboration (inside and outside the organization) to address a problem;
- Resource coordination, logistics and support capabilities;
- Identifying potential threats;
- Response measures;
- The cooperation capacity, the level of cooperation between different units, the operability and usability of communication tools and information systems in the event of incidents, the capability to view the common picture, the operational readiness, the best practices.

Through the "CYBERWINTER 2011" the participating units from different sectors have gained the following benefits:

- The players identified interdependencies that they did not suspect to exist;
- Gained experience, working with employees in their positions, but from other units;
- Shared good procedural practices;
- Checked the procedures whether were working well in practice;
- Checked the contact information and communication channels in the various units;
- Demonstrated a level of preparation to leaders and supervisors.

Breaches in information security aimed at verifying the readiness of the expert and management staff to perform the following activities:

- Identify the occurrence of an incident;

- Take first response actions trying to mitigate data loss or other irreversible damages in the information systems, as well to close the system gap if that is the reason for the incident occurrence;
- Make damage assessment, and identify all details of the incident;
- Prepare a recovery plan;
- Recover the hacked system.

The CAX "CYBERWINTER 2011" is a part of ENISA's research and analysis of national and international cyber exercises carried out. ENISA examined 85 exercises covering the period between 2002 and 2012. In total, 84 countries worldwide participated in the multinational exercises. A total of 22 European countries conducted in national cyber-exercises.[11]

The "CYBERWINTER 2011" is a first initiative to cyber security capacity building through CAX. This established a base of common understanding for the importance of maintaining high staff readiness to identify cyber risks, to respond and recover the information systems. The CAX highlighted the need to increase a focus of on CAX implementation in Public sector, creating a CAX management model, developing tools and methodologies for both planning and improved from future exercises.

Other lessons learnt from the exercise are:

- Cyber security is an urgent matter;
- Cyber crisis public organizational cooperation efforts have to be continuously developing;
- There is a need to intensify public–private cooperation in cyber exercises. Public-private partnerships during cyber exercises are essential;
- More attention should be paid to developing exercise management tools which can support exercise execution and preparation;
- The use of methodological planning, monitoring and evaluation is crucial for effective exercises;
- There is broad consensus that cyber exercises help to enhance the preparedness, responsiveness and knowledge of stakeholders in responding to cyber incidents.

Cyber NRA 2014
National Revenue Agency

On 07-09 May 2014, National Revenue Agency in Bulgaria conducted CAX for cyber security – Cyber NRA 2014. The CAX goals were to enhance the capabilities of responsible experts in NRA to protect the information and communication infrastructure against cyber-threats and information security breaches. It aimed to identify organizational and technical vulnerabilities in the system for information security management and in the procedures and policies for responding against cyber incidents occurrence.

Due to the specific of the agency's activity, any further detailed information about the CAX Cyber NRA 2014 is confidential.

MT CybEx 2016
Ministry of Transport, Information Technology and Communications

On 27 - 28 October 2016 regarding the contract: “Analysis and adaptation of EU and NATO models for the purpose of updating the existing model in MTITC for planning and conducting cyber security computer assisted exercises. Planning, preparation, conducting and analysis of cyber security training in MTITC and the second-level spending units to the Ministry,” a Computer Assisted eXercises (CAX) in Information Security MT CybEx 2016 was accomplished.[12] It is a ‘Operational’ level exercise. The main purpose is to verify the existing Standing Operating Procedures (SOPs) and specific measures or processes that need to be taken when cyber incidents occur in the organization. These measures include co-operation and coordination between the organization's units and beyond. The Cyber CAX at MTITC was held on an EU and NATO model (Cyber Europe, Cyber Coalition, Locked Shields, Cyber Atlantic 2011, Cyber Storm, etc.). The preliminary work for the exercise lasted 5 months.

A specialized technology platform - CEP EXONAUT Suite platform[13] was used for the MT CybEx 2016. With the help of the software solution EXONAUT, every event, incident, injection, communication, actions and response undertaken by the participants was traced, evaluated in real time, recorded and stored for the purpose of subsequent analysis and lessons learned. It has been drawn up in line with the requirements and policy in the area of network and information security of European Union.

EXONAUT in MTITC (Fig. 5) is composed of various functional and technically compatible modules integrated with each other - CPM – Compliance and Performance Manager, OBS – Observer, TDE – Tactical Data Editor, и TEM – Training and Exercise Manager.

Under the scenario, players work for the administration of an illusory country called Bulland, which experiences migration pressure and faces presidential election as well as the Presidency of the Euroland Union.

The training began with an announcement in the social network by the terrorist organization Cyber dominant about imminent attacks on the cyber security of Bulland. The role of the “good ones” in this scenario played employees of MTITC as seven external IT experts assumed the role of the leader of the terrorist organization Al Hacker. Eleven incidents were planned for the event – 6 for administrative experts and 5 for IT experts. During the CAX were played: for administrative experts – 4 incidents and 15 injections; for IT experts – 3 incidents and 18 injections.

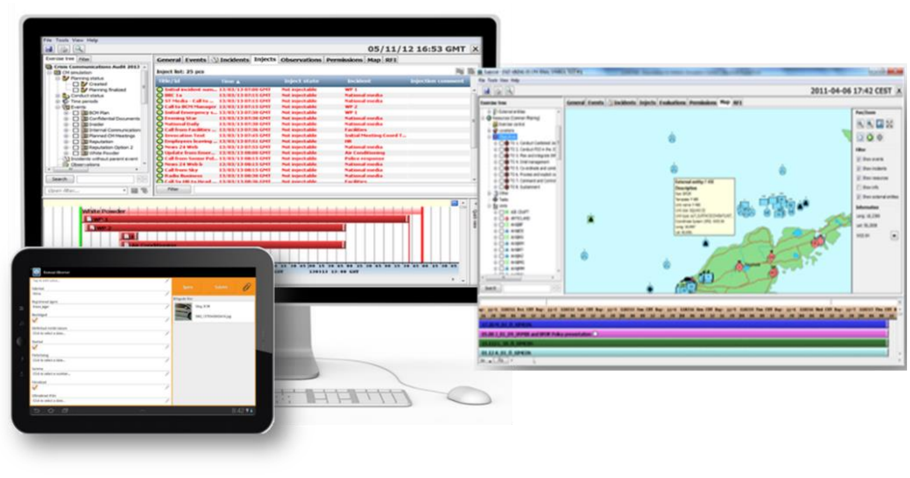
05/11/12 16:53 GMT
General Events Incidents Injects Observations Permissions Map RFI
White Powder
2011-04-06 17:42 CEST

Figure 5: EXONAUT – TEM.

Within the project framework, a set of theoretical and practical trainings and demonstrations were held before the CAX. The first group of trainings was designed to present the contemporary challenges to global information security, discussing and demonstrating key issues in cyber security and addressing threats. The second part of the training was aimed at acquainting the participants with the ENONAUT technology platform for planning, conducting and analysing the exercises.

Participants

MT CybEx 2016 was attended by more than 60 participants from Bulgaria and abroad, functionally divided into four teams:

1. *EXCON* – Centre for exercise management – CAX management, assessment and control. The Director of exercise and his team were managing, tracking, and evaluating in real-time the occurrence of scenario events, directing injections, observing the actions of the participants in the planned incidents, as well as overall dynamics, adding changes in the course of the exercise.
2. *Training audience* – separated into two operational centres, Administrative experts and Experts – Information Technology.

- MTITC;
- Executive Agency "Electronic Communication Networks and Information Systems";
- Executive Agency "Automobile Administration";
- Executive Agency "Railway Administration";
- Directorate General "Civil Aviation Administration";

- Executive Agency “Maritime Administration”;
- Executive Agency “Study and Maintenance of the Danube River” – Ruse;
- CERT-Bulgaria - National Computer Security Incidents Response Team;
- National Transport Hospital – Sofia;
- National Transport Hospital – Plovdiv;
- Air Squad 28.

3. *Observers and VIP guests* – representatives of the European Network and Information Security Agency (ENISA), the Ministry of Defence, NATO Centre of Excellence in Crises Management and Disaster Response, the National Revenue Agency and the State Agency “National Security,” media, etc.

MT CybEx 2016 results

The CAX assessment contained two parts – real-time and after action review based on developed methodology. Assessment criteria applied to the exercise included the level of compliance with ISO 27001.The real-time assessment described above enabled the initial results of the player’s performance in the development of the scenario during and after the exercise as well. The visual representation of the results was presented through the EXONAUT Compliance and Performance Manager module. Exonaut CPM (Fig. 6) allows users to create exercise campaigns where the organisational entities and training objectives are imported into Exonaut Training Progression Manager (TPM) from Exonaut TDE, which acts as the central repository for this data. After mapping the training objectives in the TPM the exercise campaign is synchronized to TEM where each exercise is planned and delivered. The observer client is used to observe and assess the performance of the organisational units during the exercises against the objectives that have been set. All this creates a summary assessment for

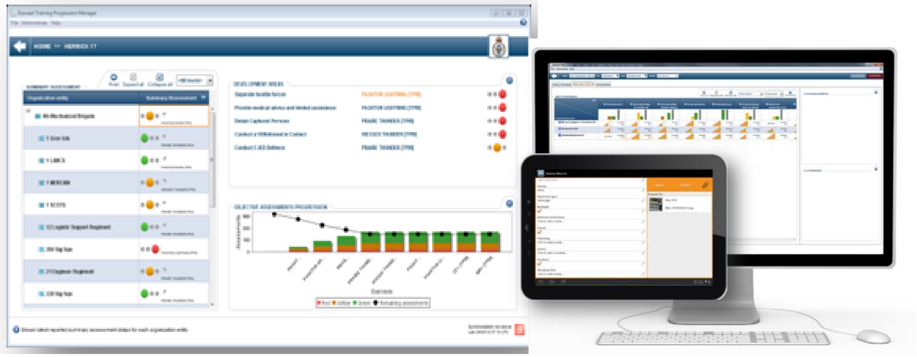

Figure 6: EXONAUT CPM.

the organisational units after an exercise, based upon the results of the objective assessments. As a result of this process a dashboard screen highlights exercise results, exercise areas that need extra training and a progression summary for the exercise campaign.

The detailed analysis of the collected information and the results of the MT CybEx 2016 showed that initially planned goals have been achieved.

The recommendation is that similar exercises should be repeated periodically to update employee's knowledge and preparation to act on cyber incidents.

The main lesson of the MT CybEx 2016 is that by applying a complex approach to the process of increasing the human resources qualification, organizing trainings ending with exercises, we enable the practical application, experimentation and validation of the knowledge acquired at the training stage and the effectiveness of whole training increases many times.

Such type of computer assisted exercises need to be carried out every year, covering different levels of training audience, in order to upgrade the acquired qualification and application of real models.

Conclusion

Cybersecurity exercises aim to increase the level of understanding of the cyber environment and the resulting threats in organizational, national and international terms (including legislation) and the need for capacity building and collaboration. The successful application of Computer assisted exercises in cyber security management and the improvement in the preparation and qualification of staff members could enable various scenarios analyses, put the focus on preventive actions and enhance decision-making during cyber incidents. The analysed information allows higher precision in risk and impact assessment of incidents and increases the effectiveness of the recovery activities.

Broad use of the CAX model by the conducted exercises in the Public sector can support organizations in evaluating and improving their cybersecurity programs, procedures and cybersecurity capabilities development. The model focuses on the CAX implementation and management of cybersecurity trainings and exercises associated with the information and communication technologies assets and the environments in which they operate.

Regularly holding CAXs specific for the needs of cyber security preparedness would provide a new comprehensive training and analytical capability for Public administration. Training methods aiming to ensure maximum results with the use of minimum resources, are consistent with the requirements for speed, precision and flexibility.

Forward-thinking organizations are adopting a new model for cyber-security trainings with a trend of transition into a Cyber CAX Service Model. Building on successful implementation of the approach to run CAX as a project[14] we have learnt a lesson that regularity and spread of Cyber Resilience CAXs among different administrations in the Government and local authorities requires to develop a model for Cyber CAX as a service. Other important lesson is that using adequate platform for automation of the CAX provides opportunity to focus on scenario and data, that are specific to different training audiences. Specializing in using most effective way the CAX platform makes it possible for a small external team to support exercises in many administrations the most cost effective way, when the scenarios and data rest with the administrations as an ownership and responsibility. So Cyber CAX as a service is actually shared service for administration that provides effectiveness, efficiency and savings in Cyber training.

Further unification of Cyber CAX service will give an opportunity in addition to training domain to use these CAXs for formal certification and in support of accreditation of cyber domains of different administrations in the process of their federation for the e-Government infrastructure / services.

As a result, cyber-security leads to innovations. The new approach includes best practises, established methodology for CAX planning, conducting and evaluation, real-time monitoring, controlled training environment, advanced tools and special software.

Acknowledgement

Finally, I wish to thank all people and organisations, which have contributed to the exercises as well as the project management teams form MTITC and NRA who made CAXs successful.

Notes:

[1] Razvan Gavrila, ed., *The 2015 Report on National and International Cyber Security Exercises: Survey, Analysis and Recommendations* (Heraklion, Greece: ENISA, 2015), available at https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises/at_download/fullReport.

[2] Gavrila, ed., *The 2015 Report on National and International Cyber Security Exercises*.

[3] Erdal Cayirci and Dusan Marincic, *Computer Assisted Exercises and Training: A Reference Guide* (Chichester, UK: John Wiley, 2009).

[4] *Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks* (Heraklion, Greece: ENISA, 2009), available at www.enisa.europa.eu/publications/national-exercise-good-practice-guide/at_download/fullReport.

[5] Irena Nikolova, *Computer Assisted Exercise Management Environment for Civil Security*, PhD Thesis (Sofia: Institute of ICT, 2011).

[6] Ognyan Kounchev, Rene Willems, Velizar Shalamanov, and Tsvetomir Tsachev, eds., *Scientific Support for the Decision Making in the Security Sector* (Amsterdam: IOS Press, 2007).

[7] European Commission, DG ECHO, *Exercises: Archives*, available at http://ec.europa.eu/echo/files/civil_protection/civil/prote/exercises_archives.htm.

[8] *Computer Assisted Exercise Phoenix 2010*, Sofia, Ministry of Defence, available at http://phoenix.mod.bg/index.php.

[9] *4C Strategies*, https://www.4cstrategies.com/.

[10] *CyberWinter 2011 Exercise*, Sofia, Ministry of Transport, Information Technologies and Communications, available at https://www.mtitc.government.bg/page.php?category=583.

[11] Panagiotis Trimintzos and Razvan Gavrila, *On National and International Cyber Security Exercises. Survey, Analysis and Recommendations* (Heraklion, Greece: ENISA, 2012).

[12] "We shouldn't ask ourselves whether cyberattacks will occur, but when and how ready we will be," Sofia, Ministry of Transport, Information Technologies and Communications, available at https://www.mtitc.government.bg/bg/category/1/zamestnik-ministur-valeri-borisov-ne-biva-da-si-zadavame-vuprosa-dali-kiberatakite-shte-se-sluchat-koga-i-kolko-podgotveni-shte-budem (in Bulgarian).

[13] *4C Strategies.*

[14] Nikolova, *Computer Assisted Exercise Management Environment for Civil Security*.

About the author

Dr. Irena Nikolova is an economist, researcher with more than 20 years of experience in the field of defence and security economics, crisis management, project management, economic analysis, computer-assisted exercises, trainings, analysis and assessment of lessons learned.

She holds a PhD degree in Automated systems for information processing and control, specialised in the fields of project management, marketing, training and customer support. She participated in several projects for modelling and simulation in the area of civil protection and defence. She worked as a senior adviser to the Ministry of Defence in the frame of project management of science, technology and procurement system, a basis for the PRINCE II methodology.

She has a number of publications in the field of financial management of research projects, economic analysis, development of the Balanced Scorecard for assessing performance, optimization, planning and developing systems for crisis management and computer-assisted exercises.

Irena is a member of the Bulgarian Modelling and Simulation Association – BULSIM and expert "CAX Management and Planning" of CYBER WINTER 2011, Cyber NRA 2014 and MT CybEx 2016.