Information & Security: An International Journal

T. Tagarev, G. Sharkov, and N. Stoianov, vol.38, 2017, 93-108

https://doi.org/10.11610/isij.3807

CYBER SECURITY AND RESILIENCE OF MODERN SOCIETIES: A RESEARCH MANAGEMENT ARCHITECTURE

Todor TAGAREV, George SHARKOV, and Nikolai STOIANOV

Abstract: Advanced information and communications technologies (ICT) facilitate the increase of effectiveness and efficiency of defence and security organizations, governmental services, the economy, and quality of life, while at the same time providing opportunities for malicious actors to cause significant damage without exercising physical coercion. Policies for security and resilience of modern societies to threats and risks from the cyberspace account for foreseen cyber threats, their immediate impact on ICT infrastructure, consequent effects on critical services, as well as cascading effects across systems and infrastructures. This paper presents the architecture used to plan and, consequently, manage cybersecurity research in Bulgaria. It covers five application areas (information management systems; industrial control systems; unmanned and remotely piloted vehicles; bio-integrated systems; and cognitive processes and decision-making), the study of systems of systems, and support to the formulation and implementation of cybersecurity policy.

Keywords: cybersecurity, resilience, ERP, industrial control systems, drone, UxVs, bio-integrated systems, systems of systems, comprehensive approach, R&T management.

1. Introduction

Wider, deeper and rapid implementation of evolving information, communications, and sensor technologies has profound effects on our economies, the functioning of governments, and our everyday lives. Central and local governments provide an increasing number of electronic and online services to companies and citizens. Defence, law enforcement, intelligence services, and crisis management in natural and manmade disasters also depend on data repositories, smoothly functioning communications networks, and collaborative decision-making.

Industrial processes and business services rely increasingly on integrated sensors, automation, remote monitoring and control. In delivering their products and services, businesses depend on cross-border supply chains, often spread over more than one continent. Drones and unmanned vehicles—autonomous or controlled remotely—are not an exotic feature of the battlefields anymore. They find innovative and ever wider applications for security purposes, transportation, service delivery, leisure, etc.

Billions of devices are already connected to the Internet, and their numbers may approach one trillion by 2025, fusing the physical and virtual worlds. This 'Internet of Things' (IoT) impacts diverse and multiple fields, affording implementation of concepts such as "smart cities" or "personalized healthcare,"[1] the latter envisioning incorporation of multiple sensors, communications devices and actuators in the human body. Easier access to online information changes the way in which we see the world, and others see us. People spend longer hours devouring and generating information in social networks, or using Internet as a medium through which they access more traditional media.

All these developments change the way in which a person in a modern society works, lives, and perceives the world, and facilitate the increase of effectiveness, efficiency, and quality of life. On the other hand, the increasing reliance on sensors and sensor networks, communications and navigation infrastructure, data and information sources introduces vulnerabilities that can be exploited by malicious actors via cyberspace, i.e. without physical coercion.

Formulation and implementation of policies for security and resilience of modern societies to threats and risks from the cyberspace require a comprehensive understanding of the threats, as well as their immediate impact on the information and communications technologies (ICT), consequent effects of infrastructures and services that are critical to society, and the cascading effects as a result of interdependencies among systems and infrastructures. The Bulgarian Defence Institute (BDI), in close cooperation with the European Software Institute–Eastern Europe, undertook the development of the respective comprehensive concept, intended to plan and, consequently, manage cybersecurity research in Bulgaria.

The article presents this concept, outlining in the next section the research management architecture. Section 3 provides information on research plans in five application areas: information management systems (IMS); industrial control systems; unmanned and remotely piloted vehicles (UxVs); bio-integrated systems; cognitive processes and decision-making. Section 4 then examines research tasks supporting the understanding of mutual dependencies among systems of systems, while section 5 deals with policy and management aspects.

2. Outline of the Research Management Architecture

The research plan pursues three broad goals:

A. Develop, test and certify products, systems, and cybersecurity solutions.

B. Support the formulation and implementation of organisational and national cybersecurity policies, as well as national positions on related international initiatives.

C. Develop and maintain adequate research capacity.

The achievement of these goals requires:

1. Understanding the evolving threat landscape;
2. Identifying vulnerabilities to cyber threats of systems and services with critical importance to national security, economy, and life;
3. Estimating the impact a cyber threat would have on an organisation, governmental functions, economic and service sectors, or life;
4. Evaluating the performance of potential or actual cybersecurity solutions and the impact they will have on security and resilience.

Requirement 1 is typical for the community of cybersecurity experts; however, requirements 2, 3 and 4 can be met when expertise in cybersecurity is combined with knowledge of the underlying natural laws of physics, chemistry, biology and physiology; psychology, behavioural science, sociology, etc., thus allowing to estimate vulnerabilities and the actual or foreseen impact of disruption of ICT on the respective sector.

Hence, the first five building blocks of the research management architecture (Figure 1) are:

- Information Management Systems, where data, information, connectivity, information flows and decision support systems are the key assets;
- Industrial Control Systems, where ICT interfaces with heavy physical and chemical processes;
- Unmanned—autonomous or remotely controlled—vehicles (UxVs) with various applications, where the behaviour of the vehicle depends on the integrity of information from multiple sensors, communications links, navigation infrastructure, etc., and the understanding of vulnerabilities and impact feeds on knowledge on how UxVs are integrated in general transportation flows;

- Bio-integrated systems, where ICT builds on advances of nano-technologies[2] and interfaces with physiological processes;
- Cognitive processes and decision-making experience increasing impact of electronic information sources, online social networks, and immersive/ virtual realities,

and may be subjected to intentional manipulation of perceptions, individual and group behaviour.

In practice, none of these areas function in isolation. Various interfaces and interdependencies exist, and disruption in one sector or system may have significant cascading effects in others. Therefore, the block “Systems of Systems” provides for research on interdependencies, supply chains, etc., and thus of understanding the full impact of a certain threat on the society.

The comprehensive understanding of threats and risks, provided in the first six building blocks, serves to define policy (organisational arrangements, procedures, priorities, resource allocation, required competences and capabilities) and manage cybersecurity research respectively.

The following three sections provide a more detailed examination of these building blocks.

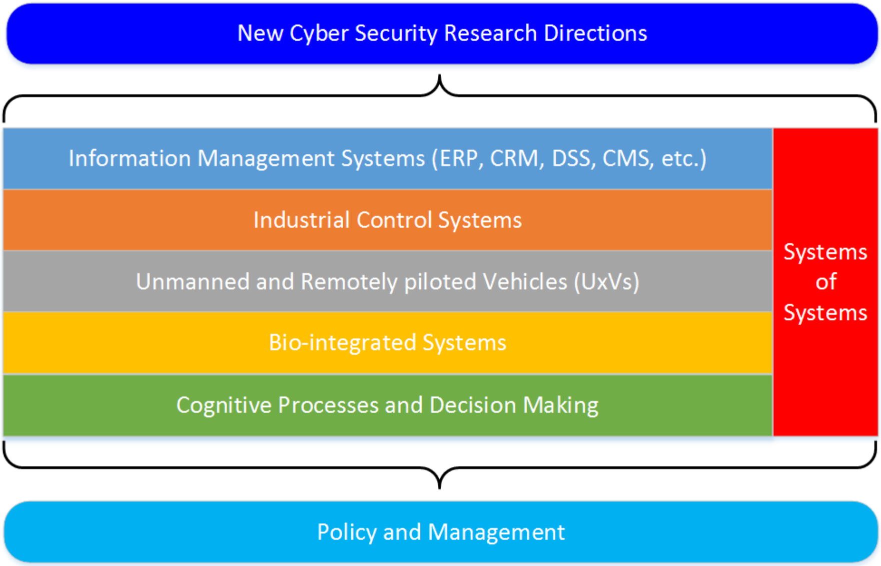
New Cyber Security Research Directions
Information Management Systems (ERP, CRM, DSS, CMS, etc.)
Industrial Control Systems
Unmanned and Remotely piloted Vehicles (UxVs)
Bio-integrated Systems
Cognitive Processes and Decision Making
Systems of Systems
Policy and Management

Figure 1: Cybersecurity Research Management Architecture.

3. Application Areas

The first five building blocks reflect the application of advanced ICT in areas that are critical for the functioning of the state, the economy, life, and decision-making.

A. Information Management Systems

Information management systems are nowadays everywhere. We use these systems to manage our relationship with customers, to plan different resources, to support decision making, etc.[3] Every organization has its own information system or systems that support organization's management. Cyber-attacks are mainly focused on such kind of systems. Attacking and stopping this type of systems can affect the whole organization, to interrupt business processes or allow attackers access to personal or other sensitive data.[4]

These systems are very likely targets of cyberattacks. One of the strands of work within the cyber security and resilient architecture will be studies of information management systems, attack profiles, vulnerabilities, existing and prospective protection tools and procedures. A new general model for this type of system will be developed and tested. Based on the analysis and tests evaluation of the currently implemented system will be made and additional cyber security measures will be applied.

Measuring efficiency and effectiveness of the cyber defence of the systems is one of the task to be addressed. To make this appropriately, a model of cyber security metrics will be developed.

The main research direction in this area is to study and analyse cyber-attacks against information management systems at tactical, operational and enterprise level, including government, bank, telecommunication, e-government, and crisis management sectors. The following research tacks will be performed in this block of the cyber security and resiliency architecture:

- Assessment of the threats to Information Management Systems;
- Study and analysis of cyber vulnerabilities inside Information Management Systems (IMS);
- Development of new methods, models, and tools for cyber security and resilience of IMS;
- Enhancing the existing research infrastructure with focus on modelling of IMS, prototyping and testing cyber security solutions.

The anticipated results include development of new models, tools and techniques, and their application in Information Management Systems. The different approaches for cyber security and cyber resiliency of such systems will be tested and evaluated. The information systems studied in this block are:

- Enterprise Resource Planning (ERP) systems;
- Customer Relationship Management (CRM) systems;
- Decision Support Systems (DSS); and
- Crisis Management Systems.

B. Industrial Control Systems

The EU Directive on critical infrastructure protection[5] examines two sectors of critical infrastructure – *energy* (infrastructures and facilities for generation and transmission of electricity; oil production, refining, treatment, storage and transmission by pipelines; gas production, refining, treatment, storage and transmission by pipelines, and LNG terminals) and *transport* (road, rail and air transport, inland waterways, ocean and short-sea shipping and ports). The 2005 Green Paper of the European Commission and a number of national documents add to the sectors of critical infrastructures chemical and nuclear industries, the provision of food and water, space and other industrial sectors.

Since Directive 114 was adopted, the dependence of these infrastructures on ICT increased significantly, as well as the vulnerability of industrial control systems to attacks via cyberspace. There is a growing body of evidence that a number of actors—some private, others state-backed—have both the motivation and the means to cause significant damage to industry and related services. Among the well-known examples are the destruction of nuclear centrifuges at the facility in Natanz, Iran by the Stuxnet worm, the follow-up attack on Saudi Aramco by Shamoon spreading to other oil and gas companies,[6] and the more recent attacks on Ukraine's power grid.[7]

This block in the research architecture is dedicated to the study of sector-specific cyber threats, assessment of vulnerabilities and the impact of cyberattacks on the sector, prototyping, testing, and certification of cyber security solutions.

C. Unmanned and Remotely piloted vehicles (UxVs)

Since 2013 the development of unmanned vehicle systems (UxVs) and drones significantly accelerated. New control systems are implemented, and geolocation and GPS positioning became part of the UxVs. Researchers and developers now use commercially available operating systems (OS), positioning applications and communication protocols. Some of these systems use Linux or Android based operating systems. The OS as a system is cyber secure but implementation and setup of the application and

OS need to be tested. The used communications protocols are not widely explored and there are publications pointing to the possibility of cyberattacks.[8]

On the other hand, drones and UxVs become cheaper and more accessible. Using such systems to attack various assets and infrastructures turns into a likely scenario.

The focus of research is now moving from the design and production of UxVs and drones to the creation of new methods for communication, control, and guidance. The provision of cyber security of all these new methods becomes one of the primary goals.

Research in this block of the architecture is focused both on cyber defence of UxVs and the protection from such systems. That includes:

- Identification and systematization of cyberattacks against UxVs and drones;
- Study, assessment and evaluation of existing methods for cyber security;
- Gap identification for the cyber security and resiliency of UxVS and drones;
- Development and testing of new methods and tools for cyber secure UxVs and drones.

The new research directions in the UxVs block of the Cyber Security Research Architecture are:

- Study of the cyber security and resiliency of the real time and close to real time applications and operating systems, implemented in the UxVs and drones (single on chip/module on chip);
- Testing and validation of communications protocols, firmware and detection of friendly forces (from cyber security point of view);
- Integration of the information from UxVs and drones with other devices (IoT support) and cloud computing;
- Detection and management of swarms.

D. Bio-integrated Systems

Modern medicine is constantly trying to improve the quality of life of patients using different hospital systems, e.g. life support systems, monitoring of biometrics, implanted medical devices and others. For example, each year worldwide, thousands of patients are subjected to interventions to implant a number of devices such as pacemakers, implantable cardioverter defibrillators, spinal implants, neurological devices, insulin pumps, and others. In addition to the conventional use, these devices offer an opportunity to monitor the condition of patients.

Despite the relatively high degree of security and reliability of the devices achieved in recent years, these devices—and any in-formation-operated hospital system—may be subjected to cyber abuse. In this respect it is important to investigate potentially vulnerable systems and the nature of cyber threats[9] and analyse the danger of malicious interference in information and control systems, as well as to develop enhanced methods of protection.

The main research goal in this block is to model threats to cyber-security of bio-integrated systems (in hospitals and personal life support systems) and seek opportunities for their protection from external and internal threats. The following research directions support the achievement of this:

- Analysis of threats to cyber-security of bio-integrated systems, taking into account the emergence of new threats;
- Development of methods and algorithms for cyber protection of bio-integrated systems;
- Development of models and testing the cyber-security of bio-integrated systems;
- Cyber security of hospital monitoring systems, biometrics;
- Cyber security of hospital systems for life support;
- Cyber security of the hospital systems for emergency life-saving interventions;
- Cyber security and resiliency of the personal life support systems (implanted/ implantable medical devices, or IMD);
- Cyber security of the public funds for emergency life-saving interventions (e.g. disposable defibrillators).

Research in this block is applicable to the study of advanced soldiers' systems. Further, and depending on the evolution of integrated systems, it may be extended to cover the cyber security of animals and plants.

E. Cognitive Processes and Decision-Making

Protecting decision-makers and social cohesion has always been an important security objective. Advanced ICT provide qualitatively new opportunities to influence perceptions. We often rely on decision-makers taking rational decisions, while in fact there are numerous cognitive biases that put a strain on the rational choice theory[10] and can be exploited by a skilful and motivated actor. News in the form of text, images, or video, especially when they are part of a sustained campaign, can significantly influence individual cognition, perceptions, peer pressure and, as a result, lead to intended behaviour and cause significant damages.

The study of cognitive processes and decision-making requires integration of IT expertise with knowledge in the fields of psychology, behavioural science, anthropology, and sociology in order to understand vulnerabilities, mechanisms of impact, and devise protective measures.

4. Systems of Systems

The modern digitized world is operated by complex and interconnected systems. To cope with that complexity for the last decades the notion of systems-of-systems (or SoS) was introduced and largely exploited and developed. The SoS approach provides an adequate framework for the holistic view on cyber security and resilience of the digital ecosystems. We believe that following the generic SoS architectures and engineering principles allow to address the "cyber terrain" in depth and structure adequately the knowledge, research work and practical implementations.

A. The Systems of Systems Approach

The Systems of Systems (SoS) approach addresses conceptually new emergent properties of a complex composite system which are more than just a sum of the functionalities of the constituent systems. The constituent systems could vary according to their nature, purpose and level of digitization, though they are normally designed and able to operate independently. However, their interactions and interoperability bring a higher level of behavioural and operational dynamics that must be considered and understood by stakeholders. The SoS approach brought also a new view on the complex digital ecosystems development, where all aspects— technology, policy, economy, society, etc.—must be addressed. The heterogeneous nature and complexity of the constituent systems, which on their turn could be complex systems-of-systems, require various design and architecture solutions, tools and methods. The penetration of such embedded layers of constituent systems could go down to various 'intelligent' components, massively invading the industry (ICS/SCADA with numerous PLCs, or IIoT – industrial IoT), business management systems, security and defence systems, our 'smart' homes and life. Some of the SoS are designed and developed to support entirely virtual (digital) businesses, others provide irreversibly digitized services, scaling from e-government to bio-integrated or bionic replacements. Yet, the connectivity to the 'real world' requires the introduction of the cyber-physical ecosystems view. Therefore, the security, stability and resilience of SoS are inevitable part of their design principles, architecture and engineering requirements, and behaviour management.

1) Application in defence systems

The U.S. Department of Defense (DoD), for example, requires the use of the DoD Architecture Framework (DoDAF) in development of DoD architectures, which is essentially a framework for SoS design and engineering. SoS provides capabilities beyond what the systems working independently can provide. Resiliency of the SoS is becoming increasingly more important and necessary for mission success. Resiliency can be defined as the ability of the SoS architecture to defend against emerging threats. This defence means adapting the SoS architecture to handle the new threat. As a new threat is detected, the SoS architecture evolves into a new SoS that is resilient to the new threat.

2) Interoperability layers of SoS and security

The backbone of the SoS is the interoperability of the constituent systems. However, this interoperability should be considered at several levels and not limited to a 'system' data/ network interface levels. Among the popular frameworks that define the levels of interoperability is the Interoperability Framework of the NCOIC (Network Centric Operations Industry Consortium), tailored for military applications.[11] The framework covers three broad levels for interoperability with respective layers, as follows:

- Network Transport – physical connectivity and network interoperability;
- Information Services – data/object models, semantic/ information interoperability, knowledge and awareness of actions interoperability;
- People, Processes and Applications: aligned procedures, aligned operations, harmonized strategy/doctrine, and political or business objectives.

Respectively, the holistic approach to security and reliability of the SoS requires appropriate considerations and measures at each layer to achieve the SoS shared goals.

3) Reliability of SoS and cyber security and resilience

Some key consequences of the loose SoS architecture and interoperability affect directly the composite reliability and security, such as: dependent and cascading failures, complex event processing, chaotic behaviour, scale-free phenomena, weak coupling, weak signals. The 'emergent behaviour' of SoS capability, by definition, makes use of the capabilities of more than one constituent system to meet a demand. So, the SoS attributes emerge from the interaction of the constituent system. Therefore, the SoS reliability is normally independent of constituent system reliabilities – the SoS might be more reliable than its constituents (because of better backup capabilities), or it could be less reliable (because of the poor information exchange). The assessment and reliability (resilience) of the emergent properties becomes even more difficult if we consider the different configurations or states that may emerge dynamically in practice. To address that, the IEEE Reliability Society has decided to set up a Technical Committee on systems of systems, to assess the importance of systems of systems for reliability and dependability (RAMS: Reliability, Availability, Maintainability and Safety). Our goal is to align with RAMS the cyber security and resilience view, as it maps logically to the principles of cyber/information security and resilience.

B. Cyber-Physical Systems Models

The Cyber Physical System (CPS) is a novel framework to deal with the large-scale and mission-critical SoS implementations in their entire complexity and depth. CPS are large scaled, closely integrated and heavily resource dependent collections of distributed constituent cyber and physical systems. In CPS, the physical systems and respective processes are monitored and controlled by the computation devices through communication channels/networks. Usually, the physical devices alone have very limited computational and communication capabilities to support autonomously critical applications or functions. New architectures and interoperability models are widely used to overcome these limitations and achieve flexible and efficient SoS, such as Service Oriented Architecture (SOA), cloud computing systems and architectures. The U.S. National Institute of Standards and Technology (NIST) has introduced the following definition of the Cyber Physical Cloud Computing (CPCC) architecture: "…a system environment that can rapidly build, modify and provision auto-scale cyber-physical systems, composed of a set of cloud computing based sensor, processing, control, and data services."[12] Such architectures are used in critical (essential) services such as medical devices and systems (e-health), smart transportation (intelligent transport systems, Unmanned Aerial Vehicles), 'smart' electrical power grid, navigation and surveillance applications, social networks and gaming.

The security objectives of CPS include safety, security, reliability and resilience. The typical CPS consists of three layers – control layer, transport layer and executive layer. They must be considered simultaneously when analysing the threats and risks, attacks and defences, and respective simulations. The three-layer approach of CPS allows efficient and effective testbeds construction for various mission-critical systems (such as the electrical power grid PowerCyber testbed at Iowa State University).[13]

C. Defence in Depth and Cyber Terrain

Cyber terrain is a concept developed by the U.S. Department of Defense as an updated defence in depth model. It is an extension of the classical defence in depth multi-layered model addressing the data exchange through the network (OSI layers 2, 3 and 4). The cyber terrain covers what happens when data arrive, too. It allows the view from both the defence perspective and the threat actor perspective. However, the defence in depth is not sufficient since it covers only the network layers.[14]

A new view on the entire ecosystem in depth was introduced as Cyber Terrain in order to represent the full triangle of sustainment or the three pillars of cybersecurity: People – Organizations & Processes – Technology. The new cyber terrain model defines 15 layers that allow to structure the cybersecurity knowledge and visualize the physical and logical parts of the cyber terrain. The brief presentation of the 15-layers scheme follows (Shawn Riley[15] provides also additional detail):

- Layer 0: Geographic Layer – the geographic area where real-world devices, people, organization buildings, and other physical items resides. It defines the context of the applicable cyber laws, policies, etc.;
- Layer 1: Physical Layer – the physical layer of the OSI model includes all the hardware, cables, etc. Respectively, this layer includes physical security and controlled access spaces;
- Layers 2-7: Logical Layers – Communications Ports and Protocols, i.e. the upper six layers of the standard OSI model covering communications ports and protocols of the cyber terrain;
- Layer 8: Machine Language – used to represent data such as binary executables, class files, shared libraries (e.g., DLLs), or other machines code. This includes items such as embedded system, those used in SCADA systems, BIOS, and firmware on various devices such as video cards and storage devices;
- Layer 9: Operating Systems;
- Layer 10: Software Applications;
- Layer 11: Persona – user accounts, user IDs, email addresses, phone numbers, etc.;
- Layer 12: People / Supervisory / Temporal – real-world people (the actual individual);
- Layer 13: Organization;
- Layer 14: Government.

The layers from 2 till 11 are usually referred to as a "cyberspace," but the holistic approach to cybersecurity and resilience require complex multi-layer view with respective inter-layers dependencies. In addition, the SoS interoperability is based on patterns and activities that engage multiple layers as well (thus making the threats and vulnerabilities analysis complicated and based on composite and heterogeneous parameters). Attacks and defence (response) propagate and engage numerous layers, too.[16]

D. Supply/Value Chains as Systems of Systems

The SoS approach could be particularly tailored to engage more naturally the business and industry in building the collective cyber security and resiliency derived from the standard Porter's business value chain analysis. Value chains (or value streams) provide a logical scheme to identify and engage the interconnected businesses through their normal business dependencies, roles and channels and then add the underlying digital dependency and the associated shared cyber risks. The view on value chains as SoS allow the identification and modelling of various 'hidden' threats and digital dependencies with significant potential impact on business continuity and resilience. There is no small or big in the value chain from a cyber security perspective, as 'small' data breaches of essential data could jeopardize the entire chain.[17]

E. Resilience – Protect and Sustain

Each service (operation, activity) is a (business) process based on four categories of assets: people, information, technology and facilities. And to complete the picture, one needs to add the external dependencies (like suppliers and supply chain, outsourced or insourced resources, but also the upstream in the supply/value chain). Services and operations continuity and resilience depend largely on the protection and sustainability of the assets engaged (without ignoring, of course, the design and implementation of the respective business process according to resilience requirements and principles). The principle "Protect and sustain" applies to all the components of the cyber-physical ecosystem, as well as to the entire organization, as it is defined in the CERT Resilience Management Model (CERT-RMM).[18]

5. Policy and Management

Research results in the application-oriented building blocks 1-5 and the "Systems of Systems" block allow rigorous, evidence-based formulation of a policy for cyber security and resilience. First, it provides comprehensive understanding of cyber threats and trends in their evolution. Secondly, it allows for evaluation of consequences of one or more attacks on the level of a system, a sector, and aggregated negative impact on society. Thirdly, and combining the two above, it becomes possible to implement a risk management framework, prioritise and focus available human, material and financial resources on minimising risks to cyber security.

Minimisation of risks further requires understanding of wide spectrum of approaches and capabilities, comparing preventive, protective, defensive and reactive measures, as well as measures to increase cyber resilience.

Research aims also to describe cybersecurity capabilities comprehensively, i.e. with their organisational, procedural, technological, human and training components. Of particular value is the identification of required competences, and the link that provides to education and training curricula.

6. Conclusion

The outline of a Cybersecurity Research Management Architecture was presented in this paper. The architecture consists of six elements –information management systems, industrial control systems, unmanned and remotely piloted vehicles, bio-integrated systems, cognitive processes and decision making, and their analysis in a Systems of Systems approach. Collaborative research in these fields (blocks) will result in developing cyber security policy and management view, and identifying new cyber security research directions.

For the realisation of the concept presented here, the Bulgarian Defence Institute and the European Software Institute–Eastern Europe formed a consortium with three Bulgarian universities and two institutes of the Bulgarian Academy of Sciences, as well as a number of research organisations and companies from Bulgaria and abroad as associated partners. As a whole, the consortium has the capacity needed to meet the objectives of this ambitious research plan, and adapt the research agenda to the evolving political, technological and security landscape.

Acknowledgement

This paper reflects work within procedure BG05M2OP001 of the Ministry of Education and Science of Republic of Bulgaria for the establishment of Centres of Competence in areas of smart specialization of Bulgaria.

References

[1] Sean S. Costigan and Gustav Lindström, "Policy and the Internet of Things," *Connections: The Quarterly Journal* 15, no. 2 (2016): 9-18. DOI: 10.11610/Connections.15.2.01.

[2] Adrian M. Ionescu, "Nanotechnology and Global Security," *Connections: The Quarterly Journal* 15, no. 2 (2016): 31-47. DOI: 10.11610/Connections.15.2.03.

[3] Mariano Nunez, "Cyber-attacks on ERP systems: An analysis of the current threat landscape," *Datenschutz und Datensicherheit* 36, no. 9 (2012): 653-656. DOI: 10.1007/s11623-012-0220-5.

[4] Alexander Polyakov, "Why are ERP systems an easy target for cyber-attacks?" *Cyber Defense Magazine* (June 2013): 34-35, available at www.cyberdefensemagazine.com/newsletters/june-2013/index.html#p=34.

[5] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L 345 (23 Dec 2008), 75-82.

[6] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (April-May 2013): 81-96.

[7] Ben Buchanan, "Cyber attacks on Ukraine's power grid: to what end?" *IISS Cyber security*, 3 February 2017, available at http://www.iiss.org/en/topics/cyber-security/cyber-attacks-on-ukraines-power-grid-00d9.

[8] Kim Hartmann and Christoph Steup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," in Karlis Podins, Jan Stinissen, and Markus Maybaum, eds., *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (Tallinn: NATO CCD COE, 2013), available at http://ieeexplore.ieee.org/document/6568373/;

Mike Heiges, Rob Bever, and Kyle Carnahan, "How to Safely Flight Test a UAV Subject to Cyber-Attacks," *Cyber Defence Situation Awareness Symposium* (STO-MP-IST-999), available at http://www.sercuarc.org/wp-content/uploads/2014/05/How2SafelyFlightTestUAVSubject2CyberAttacks-CSOSymposiumPaper-Heiges.pdf (accessed on 05 Feb 2017);

Konrad Wrona, "Securing the Internet of Things a military perspective," *IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 14-16 December 2015, pp. 502-507, DOI: 10.1109/WF-IoT.2015.7389105.

[9] Misty Blowers, Jose Iribarne, Edward Colbert, and Alexander Kott, "The Future Internet of Things and Security of its Control Systems," arXiv:1610.01953v1, available at https://arxiv.org/ftp/arxiv/papers/1610/1610.01953.pdf (accessed on 07 Feb 2017);

"Cybersecurity for Medical Devices: A Risk Mitigation Checklist for In-House Counsel," Client Alert 15-247, September 2015, Reed Smith LLP, available at www.reedsmith.com/files/Publication/65d1e359-2168-44e9-9b78-980ea2ebc0e8/Presentation/PublicationAttachment/45e57ded-d467-40e9-a2fa-9d3895d63788/alert15247.pdf (accessed 02 Feb 2017);

Hannah Kuchler, "Connected devices create millions of cyber security weak spots," *Financial Times*, October 23, 2016, available at https://www.ft.com/content/a63b2de8-992c-11e6-8f9b-70e3cabccfae (accessed 05 Feb 2017);

Kelly Jackson Higgins, "Hospital Medical Devices Used As Weapons In Cyberattacks," DARKreading, June 8, 2015, http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751 (accessed 04 Feb 2017);

"Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff," U.S. Department of Health and Human Services, December 28, 2016, available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (accessed 05 Feb 2017);

Patricia A.H. Williams and Andrew J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices* 8 (2015): 305-316. DOI: 10.2147/MDER.S50048.

[10] Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens, GA: University of Georgia Press, 2016);

Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Strauss, and Giroux, 2013).

[11] NCIOC, "NCOIC Interoperability Framework (NIF)," available at http://www.ncoic.org/10-news/33-tech-prod-framework-nif (accessed 4 March 2017).

[12] Tianbo Lu, Jiaxi Lin, Lingling Zhao, Yang Li and Yong Peng, "A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields," *International Journal of Security and Its Applications* 9, no. 7 (2015): 1-16, DOI: 10.14257/ijsia.2015.9.7.01.

[13] Power Infrastructure Cybersecurity Laboratory, Department of Electrical and Computer Engineering, Iowa State University, http://powercybersec.ece.iastate.edu/powercyber/welcome.php (accessed 13 April 2017).

[14] David Raymond, Tom Cross, Gregory, and Michael Nowatkowski. "Key Terrain in Cyberspace: Seeking the High Ground," in Pascal Brangetto, Markus Maybaum, and Jan Stinissen, eds., *6th International Conference on Cyber Conflict*, Tallinn, Estonia, 3-6 June 2014, 287-300. DOI: 10.1109/CYCON.2014.6916409.

[15] Shawn Riley, "Cyber Terrain: A Model for Increased Understanding of Cyber Activity," Centre for Strategi Cyberspace + Security Science, August 20, 2016, available at http://cscss.org/CS/2016/08/20/cyber-terrain-a-model-for-increased-understanding-of-cyber-activity/ (accessed 13 April 2017).

[16] Riley, "Cyber Terrain: A Model for Increased Understanding of Cyber Activity."

[17] Luca Urciuoli, Toni Männistö, Juha Hintsa, and Tamanna Khan, "Supply Chain Cyber Security – Potential Threats," *Information & Security: An International Journal* 29, no. 1 (2013): 51-68. DOI: 10.11610/isij.2904.

[18] Richard A. Caralli, Julia H. Allen, and David W. White, *CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience*, SEI Series in Software Engineering (Uper Saddle River, NJ: Addison-Wesley, 2011).

About the authors

Prof. Todor TAGAREV leads the Centre for Security and Defence Management – part of the "IT for Security" Department in the Institute of ICT, Bulgarian Academy of Sciences. He coordinated the drafting of the proposal to establish Centre of Competence on "Cyber Security and Resilience of Systems of Systems."
E-mail: tagarev@bas.bg.

Dr. George SHARKOV leads the Centre Eastern Europe of the European Software Institute and the Cybersecurity Lab at Sofia Tech park. In his capacity of National Cybersecurity Coordinator, Dr. Sharkov led the development of the first national cybersecurity strategy "Cyber Resilient Bulgaria 2020." *E-mail*: gesha@esicenter.bg.

Dr. Nikolai Stoianov is Associate Professor in the Bulgarian Defence Institute and national representative to the Information Systems Technologies panel of NATO's Science and Technology Organization. Experienced researcher and team leader, he leads, *inter alia*, Bulgaria's participation in the NATO series of Cyber Coalition exercises. *E-mail*: n.stoianov@di.mod.bg.