SECURITY OF CRITICAL INFRASTRUCTURES UNDER THE EVOLUTION OF ADVANCED TECHNOLOGIES

Benedictos Iorga

Spiru Haret University, Faculty of Engineering and Computer Science, Bucharest, Romania

E-mail: iorga.ben.mi@spiruharet.ro; iorgaben@yahoo.com

***Abstract**: The transformation speed of human society in the last decade is overwhelmingly due to technological developments, based on the artificial intelligence implementation, the global expansion of the cyber environment, the IoT emergence, and last but not least, the dual-usage operationalization of systems and technologies. The technology change has a profound impact on critical infrastructures security, both through the emergence of new threats and risk levels and through the diversification and repositioning of old threats. Thus, both technology and risk diversity carry security adaptation systems for critical infrastructures protection.*

In this context, the adaptation of security systems to new innovative technologies to ensure critical infrastructure protection becomes an almost continuous measure.

The fast understanding of amplification and diversification directions of threats and risks generated by the "twisted effect" of advanced technologies and the effective implementation of new architectures and solutions to counter security vulnerabilities manifested in critical infrastructures will differentiate between the relevance and irrelevance of integrated security systems in the future.

My current research work aims to identify the advanced technology development in the spectrum of threats to critical infrastructure security and to determine potential implementable technical solutions for an effective response to new threats amplified by the disruptive technology evolution.

Keywords: *artificial intelligence, security, integrated system, risk, threat, drones, critical infrastructure*

The impact of advanced technology evolution on critical infrastructure security

Critical infrastructure comprehensively defined by US law as ”*systems and assets, whether physical or virtual, so vital (….) that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" **[1]** has undergone a remarkable evolution in terms of extending interdependence and interconnectivity between component systems, generated by the development in information technology.

Ever since the Roman Empire, one of the most important aims of the defense system and policies has been the protection of what we today call *"critical infrastructure (CI/CNI)"* of the old empire. Roman fortresses were relying, during the glory of the empire, on a circular, concentric security system identified today under the concept of *“defence in depth”* **[2].** Thus, any Roman fortress was defended and protected by at least 4 security (concentric) rings, which had in the epicenter the “critical Roman infrastructure” represented by the governor's house and the respective Roman power centers: senators' residences, senate, forum, “*comitia centuriata*” **[3],** etc. Regardless of the defense strategies implemented or the specific techniques, ensuring the security and protection of critical infrastructure has taken precedence over any other activity, and its basis was the specialized human staff.

In today's age, governed by digital technology, ensuring the security of a state's critical infrastructure, or on a small scale, a "smart city", is no longer an exclusively human or technical task.

This implies a complex, hybrid activity carried out by specialized human factor and technical factor, based on a conglomeration of interconnected subsystems under the concept of *integrated security systems.* Security functions specific to critical infrastructure protection are ensured through specialized and dedicated subsystems, being mainly developed for the complementary counteraction of multi-spectrum threats such as unauthorized physical or logical access to infrastructure, unauthorized access to infrastructure-specific data and information, preservation of the functions of security systems /equipment that protects infrastructure, limiting and denying the critical infrastructure or related systems functionality, circumvention of security rules by staff operating the critical infrastructure, etc. In the context, advanced security systems dedicated to critical infrastructure protection may be defined as integrated systems specialized in ensuring the protection, security and active monitoring of infrastructure and its essential components aiming at maintaining basic functionalities, increasing resiliency level and prohibiting any destructive action on infrastructure elements, whether physical or logical.

The sizing, development and deployment of security systems dedicated to critical infrastructure protection are currently performed under complex security risk analysis, infrastructure reference industry case, and threat materialization impact in recent history, the evolution of security systems technology, depending on the experience of specialized personnel and not least on the ability of states to assimilate, develop and implement advanced protection technologies.

While in the past digital technology and security systems changes have gradually evolved linearly, the emergence of dual-use disruptive technologies such as autonomous platforms (underground, ground, air, sea drones), cyber technologies, cyber-attack/protection platforms, robotics, artificial intelligence, satellite surveillance systems and miniaturization of sensors will require exponential evolution of technical security systems dedicated to critical infrastructure protection, regardless of the area it serves.

Defining a security architecture in the new technological context shall consider a broad and innovative spectrum of threats, to the detriment of legislative, budgetary limitations or case-related impact. The main future features of dedicated security architecture and systems shall be "resiliency" and "adaptability" to advanced technology threat actions. While in the past the main threat to any critical infrastructure was *the human factor and its direct action*, the future threat will be *autonomous drone platforms (UAV/UAS, UNV, and UGV), intrusive cyber-systems and destructive-handling artificial intelligence capabilities.*

The evolution of security systems, from analogic to digital platforms, has taken around 20 years and has been driven mainly by the evolution of information technology and network environment. In our assessment, currently, the developmental state of security systems dedicated to critical infrastructure protection, although accelerated by technology, lies at the border between digital technology and artificial intelligence.

The evolution of dual disruptive technologies mentioned above will generate a major conceptual, operational and technical impact for integrated security systems, as follows:

a. *The expansion and miniaturization of autonomous civil-military dual-use drone platforms* will result in a shift of the threat spectrum to the critical infrastructure security, *now on the ground, to a multi-spectrum area* (underground, air, land/sea);

b. *The use of offensive cyber systems and unhindered access to intrusive cyber-assets and technologies* by non-state actors and civil companies *will increase the threat to electronic and cyber-preservation of security capabilities through remote intrusive access or direct electronic spectrum actions in the electronic spectrum on the critical infrastructure essential components;*

c. *The liberalization of artificial intelligence capabilities and the possibility of handling machine-learning algorithms will result in diversification and simplification of illicit documentation activities of critical infrastructure vulnerabilities, using the common infrastructure interconnection environment.* The future interconnection level of any critical infrastructure will increase, as the outcome of digitalization and unification of network processes and architectures across the states.

d. *The large-scale materialization of the IoT* **[4]** *concept and increase in the number of devices/equipment* dependent on an internet connection or online updates, within critical infrastructure, even in dedicated protection systems, will lead to *security vulnerability of any critical infrastructure,* without any concrete possibility of countering these threats, using current technologies and resources;

e. Wide-scale acquirement by civil entities and companies of *the capabilities to scan, observe and document security solutions dedicated to critical infrastructure protection will require the development of new protection capabilities and the scaling of security risk analysis in terms of threats.*

The five technological evolution trends rapidly developing in today's interconnected society, call for a rethink of the threat spectrum and profile towards the critical infrastructures of the states as well as the conceptual change of the current organizational mode and implementation of security solutions toward the most effective use of bilateral cooperation in the field of advanced technologies and counteracting the proliferation of disruptive effects.

Threat spectrum generated by technological evolutions in the area of critical infrastructures

a. *The duality of advanced technologies – drone systems.*

The threat footprint of disruptive technologies on critical infrastructure security, particularly on the ground, is continuously expanding, mainly due to the civil-military duality of the new autonomous platforms and systems. On the one hand, current technical systems such as autonomous drone platforms are dual and developed for civil purposes (research, medical, industrial, economic, social), but they can be used offensively, for destructive purposes through small adaptations, operationalization and implementations, to carry out destroying activities of critical infrastructure elements, particularly toward the energy distribution systems, transport infrastructure elements or communications networks. For instance, a commercial drone operationalized with artificial intelligence systems for the flight path and usually used in urban activities to determine the cadastral situation, atmospheric characteristics and terrestrial photography, can have a destructive use, by simply changing the flight path, the operating area, and by using improvised explosive devices and means.

For port-critical infrastructure dedicated to transport/storage of energetic resources, a fleet of autonomous sea platforms such as UMS oceanic/maritime research systems used successfully in ocean research and aquatic applications can be a vector of the direct threat to critical underwater communications infrastructure or energy resource transport routes. Almost identically, the emergence of nano drones, similar in size to ordinary insects, with a range of more than 30 minutes, wirelessly or solar charging, capable of transmitting images, positions and documenting a whole critical infrastructure can be a real danger for the protection and physical security of critical terrestrial infrastructure elements, without being effectively counteracted by the actual security systems capabilities.

The duality of autonomous platform technologies is a current reality that will be generalized shortly so that defining new critical infrastructure security and protection capabilities becomes a stringent necessity.

b. *The offensive network environment cybernetisation can preserve the security functions* (video surveillance, access control, and detection), *electro supply systems or SCADA* **[5]** *control systems* by advanced malware, APT-type attacks, and zero-day exploit in network equipment, IP cameras and operating systems and by the destructive use of offensive means in the electromagnetic spectrum. *During the last decade, when SCADA systems were using standard protocols and hardware/software as in administrative IT systems, differences between SCADA systems and IT systems were reduced. Also, the connectivity between SCADA systems and other systems increased* **[6, p.4].** In the technological future context, the totality of the cyber risks that are now manifested in the network environment, will migrate in the critical infrastructure security environment, generating an extrapolation of risk level.

c. IoT technology. The massive interconnection of network infrastructures supported in the future by development of 5G-technology will make critical infrastructure dependent on the connection environment and simultaneously on equipment, subassemblies and software manufacturers. Any current critical infrastructure, be it the energetic environment, transport system, financial systems or the medical

field, depends on the hardware components and software platforms. The IoT environment will generate the integration of these components with the global interconnection environment and the level of security risk will be both from the outside to the internal infrastructure environment and from inside to the outside environment. The relationship between technology manufacturers, interconnection service providers and software manufacturers will define the security level of critical infrastructures shortly, regardless of the ability of states to ensure their protection and security.

Conclusions and proposals for adaptation and development of integrated security systems

The dynamics of technological change over the last decade has left its mark on the upward evolution of critical infrastructures threats in such a profound way that the notion *adaptation* of integrated security systems will most likely be replaced in the future by notions such as *innovation and reinvention.*

The effective response to new threats is found in technology, as well as in the growth of culture and security training of specialized personnel while rethinking the security procedures. Technically, technological changes will bring about a rethink of how to integrate security systems component modules, subsystems, and a systemic change by implementing new advanced capabilities and technologies, as follows:

a. *Security system integration currently performed at the physical/network layer* (third layer of the OSI model) *needs to be performed at the application/software level of the OSI architecture*. Thus, each security system related to critical infrastructure will additionally cover the other systems in a wider spectrum of threat, and data and information obtained can be integrated, interpreted, processed and exploited centrally, thereby achieving a synergy of security functions and protection actions. Security functions interconnection at the software/application level will also enable artificial intelligence algorithms deployment to optimize threat analysis and security monitoring processes, thus excluding human subjectivity.

b. *The development of security systems dedicated to critical infrastructure protection shall be modular, using „in-house" technologies, by national industry companies* or operating in partner countries, able to ensure transparent management throughout both the production and the life cycle, while also seeking to reduce dependence on external suppliers, unknown or from states with totalitarian regimes outside bilateral alliances and agreements.

c. *The integration and interconnection of security systems across all critical infrastructures shall be a closed but extended one, meeting INFOSEC security criteria, in EAL* **[6]** standard, exclusively using a network environment, redundant, controllable, and inspected and within the protected perimeter.

d. *Video surveillance systems, control access systems to critical infrastructure elements and smart monitoring systems of all functions of critical infrastructure shall be developed in an integrated way, through the implementation of AI* „machine learning" and „deep learning" technology. Thus, the ability to document threats and limit vulnerabilities will no longer be passive but will allow identification and preemptive warning of possible threats, but also the determination of a possible pattern of their future intruding actions. For instance, the human ability to predict potential cyber threats is limited by the experience and the speed of response to the threat, but the ability of artificial intelligence algorithms to preemptively identify a potential threat or intrusive action is based on objective learning, thus increasing system responsiveness and threat identification capabilities.

e. *Physical protection and security of critical infrastructure require a rethink in terms of increasing threat identification capacity from the spectrum of physical intrusive access* to critical elements. This requires the interconnection of all infrastructure access areas through the network environment and the use of detection, recognition and identification tools enhanced by biometric technologies.

f. *The human security factor and the critical infrastructure monitoring and control systems*. The critical infrastructure monitoring and control system developed in current technologies needs to be *changed into a proactive integrated management security-critical infrastructure system*, encompassing all security components. This will allow multi-spectrum threat control and a comprehensive assessment of risk and security events. The cyber defence component will become mandatory in the future integrat-

ed security management architecture of critical infrastructure, along with the ongoing human resource training and motivation factor.

Human management and security factor will also undergo a technological process, with future protection action being a combined personal – human – autonomous platform. The level of human staff training to ensure security management will be technically high, adapted to the technologies used and the evolution of new generation platforms and sensors (cyber, autonomous platforms, artificial intelligence, software). In addition to the technological change of future technical security architectures, a procedural re-think of inter-institutional cooperation systems is required to increase the pro-activity of security platforms and systems. Thus, the critical infrastructure security cannot be ensured in the future without bilateral cooperation between states that have access to the same infrastructure or inter-institutional cooperation at the level of a state.

Providing a level of security in the future of advanced technology for states' critical infrastructures will migrate from the reactivity spectrum toward the spectrum of pro-activity and anticipation of threat evolution, to decrease the level of vulnerability by proactive neutralization of potential aggressors. The advanced technology evolution and the effects of its destructive intended use can also be countered by technology and by improving the level of training, specialization, the adaptation of staff knowledge and skills to new security systems and technology platforms.

References

[1] Section 1016(e) of the USA PATRIOT Act of 2001 - 42 U.S.C. 5195c(e).

[2] Security in depth (DID/SID)", a term derived from defense techniques that are preferentially used in the cyber environment, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[3] http://www.novaroma.org/nr/Comitia_centuriata_(Nova_Roma)

[4]https://www.internetsociety.org/resources/doc/2015/iot-overview?gclid=EAIaIQobChMIkp3U4KX66wIVRubtCh0AEwn9EAAYAiAAEgID_vD_BwE

[5] Wei & Morris, Thomas & Reaves, Bradley and Richey, Supervisory Control and Data Acquisition (SCADA). Drew On SCADA Control System Command and Response Injection and Intrusion Detection, ECrime Researchers Summit (ECrime), 2010.

[6] Kovacevic, Ana & Nikolic, Dragana, Cyber Attacks on Critical Infrastructure: Review and Challenges (draft),2015

[7] Nancy Mead, The Common Criteria, 05, July, 2013, Carnegie Mellon University 2005-2012, available at https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria