THE CYBERSECURITY OF AUTOMATED CONTROL SYSTEMS AS A KEY COMPONENT OF NATIONAL SECURITY

Galin R. IVANOV

LTC, PhD, Chief Assistant Professor,
Security and Defence Management Department,
Rakovski National Defense Academy, Sofia, Bulgaria

This article focuses on the current problems raised by the necessity to provide and ensure national cybersecurity. Moreover, it suggests measures for adequate counteraction to present-day cyber threats to automated control systems employed in the sector of national security.

Key words: *information security, cybersecurity, cyberspace, cybercrime, national security.*

1. SOME GENERAL REMARKS ON CYBER SECURITY

Currently there has been a sharp increase in cyber information security breaches which are widely spread and are acquiring threatening proportions. Many such attacks are affecting a wide range of government and private entities. The cybersecurity accidents become more frequent, more significant, and more complex and there are no borders for them. Those accidents can cause signifi-cant damages to the security and to the economy of any country, as well as to the individual members of society.

The content of the term "cybersecurity" is based on the word "cybernetics", derived from the Greek word that reads as the "science of management", namely the science for the laws of reception, storage and transmission of information, as well as artificial intelligence systems [1]. The abstract cybernetic system represents an entity of entities initially interconnected in volume that are also called elements of the system and are capable of reception, storage and procession of information, as well as information exchange.

The subject area of cybernetics and cybersecurity includes all contemporary information and telecommunication technologies. It is essential to point out that the elements of cybersecurity in the framework of the cybernetic approach are treated as intermittently interacting among each other as building elements of cyberspace as presented in **Figure 1**.

In this respect, they are:

- real time information;
- people, as active participants in the field of information exchange and use of information resources;
- software and hardware;
- global information environment.

There is a number of proven facts about cybersecurity nowadays that are worth revisiting for the purpose of this article and they are as follows:

• Cybercrime causes a wide share of accidents in the cyberspace.

• According to the World Economy Forum there is a 10-percent probability of significant collapse of critical information structure throughout the next decade which could cause damages of 250 billion US dollars.

• Eurobarometer's survey on cybersecurity in 2014 found that 38% of internet users in the EU have changed their behavior for reasons of cybersecurity: 18% are less likely to purchase goods online and 15% are less likely to use online banking. The poll also shows that 74% of respondents agree that the risk to become victims has increased, 12% have already been a victim of online fraud and 89% avoid disclosure of personal information [2].

• Every day about 150.000 computer viruses circulate and 148.000 computers are being compromised.

• According to Eurostat data as of January 2014, only 26% of the enterprises in EU have officially defined a policy about the protection of information and communication technologies [3].

• According to a research of Symantec, cybercrime victims worldwide lose about 290 billion EUR every year. Another research of McAfee indicates that income from cybersecurity are 750 billion EUR annually.

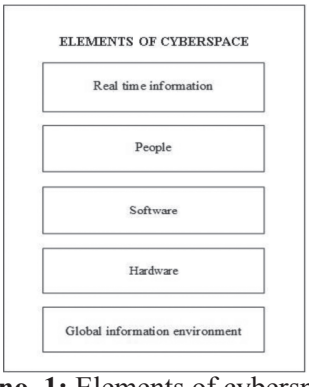

Fig.no. 1: Elements of cyberspace

All of the above considered, the main aspects of cyber threat nowadays are as follows:

• increased number of attacks, many of which lead to great losses;

• increased growth and complexity of cyber attacks that can include several levels and special methods are applied for protection against possible methods for counteraction;

• impact on almost all electronic (digital) platforms, including almost all mobile devices;

• the more frequent attacks on the information infrastructure of large corporations, important industrial sites, critical infrastructure and even government agencies with the assistance of mobile devices;

• using the most advanced countries in the field of computer technologies, through their intel-lectual resources and new cyber attack methods to carry out cyber attacks against other countries [4].

It is of paramount importance to formulate the notion of cybersecurity and to define the main goals for protection of the cyberspace and the possible arising threats. Cybersecurity at national level cannot be aimed at defending against the maximum number of threats. From a national security standpoint it is necessary to guarantee the most favorable environment for all users and systems in cyberspace, while the users, who are elements of the national security of the country, should have priority.

Cybersecurity encompasses not only classified information as an entity to be protected, but also the technical means, which are used for definition of the information

exchange among the users, the ways and the means for protection in cyberspace.

2. (NEW) EMERGING TRENDS FOR CYBERSECURITY IN THE AUTOMATED CONTROL SYSTEMS OF THE NATIONAL SECURITY SECTOR

In the contemporary environment, in order to effectively counter threats for cybersecurity on national scale it is necessary to build capabilities for symmetric response to cyber attacks or preemptive cyber strikes. The available automated systems of military and civil administration establishments need improvement by enhancing the level of automation and computerization, i.e. the building and development of automation in the protected design.

At present it is vital to review the building principles of the automated control systems in terms of ensuring the support of security in cyber space, both in peace time and in time of hostilities.

According to U.S.A. military experts in this field, on technical level comprehensive and adequate cybersecurity includes the building and use of the following subsystems:

- subsystem for defense (protection capabilities), which can guarantee shielding of the radiation of radio electronic devices and communication systems, Computer Security, Information Security.
- subsystem for detection (detection capabilities), which ensures the identifications of anomalies in the web through use of systems for detection.
- subsystem for reaction to changes in the technical parameters and conditions (reaction capa-bilities), which provides capabilities for recovery (including the reboot of part of the system) and completion of other processes and information tasks.

The evolving intelligent automated system for control in the sector of national security has to give information not only about the discovery of new and unknown cyber threats and cyber attacks in the process of surveillance (intelligence gathering) in cyberspace, but also to ensure its own cyber-security in real time, and to analyze the identified cyber threats (cyber attacks). The same should make an automatic selection of parameters for action of the automated system for control regarding degrading influence without impairment of its own characteristic features.

In the system of cybersecurity as depicted in Figure 2 , the automated system for control in the sector of national security has to feature the following capabilities:

- Automatic change of the properties and the parameters of the system and the assets for en-suring of the cybersecurity depending on the fluctuations in the state of the cyberspace (detection of activity of potential threats for cyber threats, identification of cyber attacks) and the results of the cyber attacks.
- Automatic estimation of the changes of the level of defense against cyber threats on the automated system for control in case of change of the working conditions.
- Automated decision-making for resistance to cyber attacks and automatic reaction to the sources of cyber- attacks [6].
- Automated decision-making for allocation of resources and assets for cybersecurity in case of functional

losses as a results of cyber attacks on the automated system of control.

• Forecasting, based on inherent knowledge or one accumulated in the course of exploitation, about the factors, which can influence on the level of protection of the automated system for control against all kinds of cyber threats.

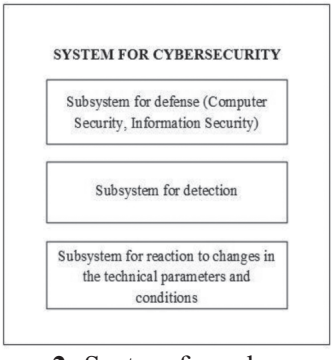

Fig. no. 2: System for cybersecurity

While defining the purposes of fight against cyber threats, we cannot reject the advancement and the application of active ways and methods, which guarantee the security of the cyberspace. That is why, with the perfection of the available automated systems for control in the field of national security a possibility should be procured for pro-active hardware and software effects (pre-emptive strikes) and active attacks against the identified sources of cyber attacks and the information systems and resources of the opposing force, as well as increase of the capacity for disinfor-mation of the opposing force as to the real characteristics and parameters of the automated system for control and its systems for security.

The most important condition for building systems for ensuring the cybersecurity in the automated control systems employed by national security is the utilization of hardware and software platforms from a trusted (authorized access) environment.

The authorization strictly guarantees the observation of the relevant requirements with regard to the Information Security, reliability and functional stability in the contemporary environments of cyber threats, while sticking to certain conditions for technological independence of the automated system for control [6].

By "trusted hardware and software environment" we understand the set of technical and program assets, organizational measures, which guarantee the building, the application and the ad-vancement of systems with special purpose, which meet the necessary requirements of the Information Security, reliability and functional stability, confirmation with certificates for compliance, in the relevant obligatory systems for certification in Bulgaria as presented in **Figure 3**.

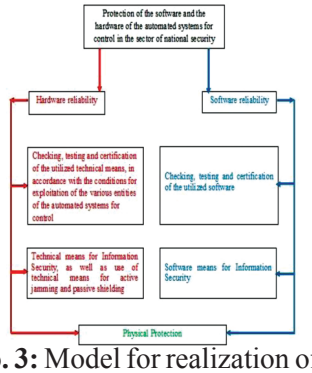

Fig. no. 3: Model for realization of cyber protection of the automated systems for control in the sector of national security

3. PROBLEMS AND POSSIBLE SOLUTIONS

Nowadays, Bulgaria's system for national security is still not ready to

a great extent for the building and the maintenance of effective and reliable protection of cyber space in the interests of the country and for effective counteraction of the constantly increasing threats for all organizations in the sector.

One of the main problems is the lack of profound scientific research on the problems of cybersecurity. A large amount of regulatory documents, doctrines and standards and other documents in the field of Information Security were developed more than ten or fifteen years ago, and they did not take into account the contemporary capabilities for leaks of information. Critical is the situation in the field of the telecommunication systems that serve the needs of the state administration and the transfer of information with limited access, built with modern imported equipment.

The automated systems for control in the field of national security, as a rule, are based on computers or based on imported components, which also creates prerequisites for preventing against the leak of information and for successfully countering the effect of cyber attacks against them.

An important characteristic in this respect is the technological delay of the Bulgarian IT industry and its dependence on international producers, which will inevitably lead to the danger of massive failures when using imported hardware and software.

The world practice in cybersecurity in the sector of national security bespeaks of the necessity of the creation of an integrated system, which combines organizational and technical security measures with the use of advanced methods for forecasting, analysis and modeling of situations. With these systems one of the main tasks has to be the ensuring the cybersecurity of the automated systems for control in the sector of the national security.

The criticality of guaranteeing the cyber defense of such automated systems for control is rendered by the damage they may suffer. Thus, the application of threats for the cybersecurity may lead to the impairment of the control function of the government and armed forces, and, therefore, to the degradation of the national security of the country and personal security of its citizens.

4. CONCLUSION

In the future it is necessary to study the main characteristics of cyberspace in detail and carefully, the dynamics of its development on different scales and to develop multi-variant procedures for its management. Without a systematic analysis and reception of realistic evaluation of the application of the security measures it is impossible to build effective systems for cybersecurity at national level.

As a conclusion, it is necessary to take the following short term and long term measures for cybersecurity improvement at national level in the sector of national security:

- Building a unified approach towards monitoring the control and defense of cyberspace in the form of a dedicated center, as well as specialized centers for counteracting cyber terrorism and cyber- attacks that rely on information and telecommunication infrastructure and inter-organizational relations to conduct their mission in this respect.

• Improvement of personnel education system including the education and requalification in the field of cybersecurity.

• Development and application of import-independent technologies, materials and components used in the building and perfection of automated system for control in the sector of national security.

• Creation of national basic information technologies, encompassing the necessary and suffi-cient set of software assets for ensuring the safe work of control automated systems in the sector of national security.

REFERENCES

[1] Bylgarski tylkoven rechnik, Izdatelstvo Zvezda, 2012;

[2] Eurobarometer's, http://www.ec.europa.eu/public_opinian/archives/ebs/ebs_390 last retrieved July 2016.

[3] Eurostat, http://www.epp.eurostat.ec.europa.eu/statistics_ehplained/ index.php, last retrieved July 2016.

[4] Galin R. Ivanov, "Cybersecurity of mobile devices". KSI Journal of Knowledge Society a publi-cation of the Knowledge Society Institute, № 1/2015, pp. 24.

[5] Galin R. Ivanov, „Konceptualni aspekti na kibersigurnostta". Sbornik s dokladi ot nauchna konferencia "Novata paradigma za sigurnost v kiberprostranstvoto", Shumen, 2014, pp.137.

[6] Parshin S., Gorbachev E., Kojanov A., Kibervoini-realnaia ugroza nacionalna bezopasnostti, Moskva, Izdatelstvo Krasand, 2011, pp. 96.

[7] P. Klimburg, et al. National cyber security framework manual // NATO CCD COE Publications, December, 2012.

[8] P. Goyal, V. Parmar, R. Rishi, Manet:Vulnerabilities, Challenges, Attacks, IJCEM, 2011.

[9] Tsv. Semerdjiev, Strategia. Sreda, resursi, sposobnosti, planirane, Klasika i stil, Sofia, 2007.

[10] J. Zachman, Concise Definition of The Zachman Framework. Zachman International, 2008.

[11] NP-06 Doctrina za KIS na Vyoryjenite sili, Sofia, 2012.

[12] NATO NAF, http://www.nhqc3s.nato.int/ARCHITECTURE/_docs/NAF_v3/ANNEH1.pdf, July 2016.

[13] NATO MIP, http://www.mipsite.lsec.dnd.ca/Pages/Default.aspx, last retrieved July 2016.

[14] DoDAf version 2.02 http://www.dodsio.defence.gov/dodaf20.aspx, last retrieved July 2016.

[15] The Common Approach to Federal Enterprice architecture, http://www.whatehouse.gov/omb/e-gov/FEA, last retrieved

[16] NATO Information Exchange Gateways Reference Architecture, March 2009, http://www.nehor.com., last retrieved July 2016.