Globalization, the State and the Individual, No 2(14)/2017, s. 263–267

Stoeva Desislava Pancheva

Doctoral candidate

Challenges to building critical infrastructure policies in a complicated cyber environment

When it comes to critical infrastructure and its protection against unauthorized access, it is appropriate to specify what definition of Critical Infrastructure (KI) is in official documents of the Republic of Bulgaria and what are the risks and threats to one of the sectors covering The critical infrastructure – its objects it. The definition of critical infrastructure is affected in several strategic documents of the Republic of Bulgaria – "Law on Disaster Protection" (ZZPB), Law on protection of classified information, "the State Agency for National Security (ZDANS). Given that critical infrastructure is a system of facilities, services and information systems, whose braking malfunction or destruction would have a serious negative impact on the health and safety of the population, the environment, national degree panstvo or on the effective functioning of government.

Critical infrastructure consists of many elements whose safe and secure operation needs to be closely monitored by the relevant authorities and institutions to avoid undesirable consequences. The term "infrastructure" was introduced in the nineteenth century by the Swiss military theorist Antouan-Henry Jominin, who emphasized its strategic and operational significance for the leadership of combat operations. Gradually, the term "infrastructure" begins to be used in economic theory and management theory.

Currently it is widely applied in computer science, economic geography and security research. At the end of the century, critical infrastructure protection was an essential element of the security policy of many countries, particularly in NATO and EU member states. This is related, on the one hand, to the process of globalization and, on the other, to the fight against international terrorism. Considering that the Republic of Bulgaria is in Europe and belongs to the EU and the EU policy on shared values, we understand that these are the major vital European interests. Using automated systems in critical infrastructure is an integral part of it in modern life, but it also makes it very vulnerable to malicious individuals, organizations, and even governments. The problem with critical infrastructure protection is relatively new. It gains a lot of international popularity in 2001

after the September 11 terrorist attacks in the United States, but this is not the first such breakthrough attempt on a critical infrastructure site to forget the 1982 case in Russia with the attack of the little-known then Trojan horse virus against the Siberian oil pipeline, as well as train attacks in Madrid on March 11, 2014. Over the years, there have been key events that have been turning points in global security. One of the most scandalous cyber-attacks against critical infrastructures in history is Stuxnet. A case with Estonia in April 2007, which is trying to purposefully block the computer network from overloading with countless false requests. This leads almost all countries, especially those at risk of terrorist acts, to initiate and make serious changes to their legislation – both in the field of critical infrastructure protection and in the direction of terrorism. As a result, the European Commission has drawn up a global strategy for Critical Infrastructure Protection, a European Critical Infrastructure Protection Program, which includes proposals to improve the prevention, preparation and response to terrorist attacks in Europe. Special programs are being developed to protect critical infrastructure, which evolve into strategic plans and even national strategies. Special attention is paid to cross-border cooperation to reduce the risk of terrorist attacks on critical infrastructure. The legal basis in Bulgaria is currently not sufficient to guarantee the security of the infrastructure; Lack of sectoral analysis The Critical Infrastructure Protection Process requires a sectoral analysis to identify the sectors and infrastructure sites that meet certain criteria for Criticality; Absence of partnership between actors in the critical infrastructure protection process, Critical Infrastructure contains multiple networks and assets united in sectors that are owned or controlled by a number of ministries, agencies, agencies, etc. On the background of dynamic growing environment and the attempt of the legislation to regulate the parameters of its functioning Republic of Bulgaria transforms in key factor for developing and supporting of strategic energy and transport objects in regional, national and international aspect. The increasing of their quantity, variety and the expanding of their areas, in combination with the higher terrorist risks, requires synchronized measures for their protection not only surveillance and early warning systems, but also means of adequate reaction. The location of critical infrastructure and its objects together with their risk assessment are made for decreasing the risk of natural disasters and protection of the population. In November 2005 European Commission accepts so called Green book for European program for protection of critical infrastructure (PCI). In the Green book for the first time on a community level is given a definition for the term "critical infrastructure" and is offered a recommended list of critical infrastructure sectors. Except for the term "national critical infrastructure", the authors of the Green book ratify the term "European critical infrastructure". For satisfactory results it is necessary to be clearly defined the tasks for evaluation and planning of critical infrastructure protection. Furthermore it is necessary to be considered the

means of critical infrastructure protecting from cyber attacks so that the practical realization of politics to respond to the expectations set in during the process of forecasting and planning. One national approach for dealing with the threats has the aim to be developed a strategy for reaction based on already made analyses and evaluations. Critical infrastructure contains systems, networks, assets and objects that provide goods and services necessary for the normal functioning of the society. The sovereignty, security and independence of the state are defined by the stable and continuous operation of critical infrastructure. Simply said critical infrastructure protection in protection of assets that are considered invaluable for the society and that provide its social prosperity. Different governments put different accents in dealing with the problems connected with CI. The aim is not to analyze and evaluate these definitions, but to highlight the accent put by governments, which highlights to form the basis of a counter-terrorism policy. "A system or parts thereof which are essential for the maintenance of vital public functions, health, safety, security, economic or social well-being of the population, and whose destruction or destruction would have significant consequences in the Member State concerned as a result of the inability to preserve those functions. "Critical national infrastructure includes those assets, services and systems that support economic, political and social life in Britain, the importance of which, if lost, could: 1. Cause huge human sacrifices; 2 to have a serious impact on the national economy; 3. Cause other serious social consequences for society; Or 3. Make immediate care of the national government" – Britain. The need to enhance critical infrastructure protection capacity is not limited to the EU and its Member States. This need is a reaction from the complex international security environment in which globalization is most clearly expressed through threats of terrorist attacks, the negative consequences of which can affect the majority of the world, taking into account the indivisible links between the states in political, economic and social terms. Cyber attacks made at the expense of modern economies materialize in a way that affects our entire modern society.

A strategic priority in national security includes infrastructures exposed to threats that may interfere with the performance of core services. The malicious code and targeted attacks aimed at sabotaging certain corporate networks are critical threats to critical infrastructure.

Oil refineries, gas pipelines, transport systems, power companies, or water supply systems control systems are all part of a technologically advanced industry where security incidents can have a negative impact on society as a whole.

In our times, we are constantly seeing an expansion of infrastructure any kind, and this expansion also increases the potential entry-point of any cyber attacks. According to cyber security experts, security is a key element of the state's national security – cyber space is a specific „virtual" territory without physical boundaries in which „democratic functioning of institutions and citizens' fundamen-

tal rights and freedoms must also be guaranteed."Cyber space is seen as the fifth domain to conduct operations against national interests, territorial integrity, national security of sovereign states, and citizens' rights and freedoms. Increasing the risks and threats in the geopolitical and strategic security environment, and in particular cyberspace, create the conditions for increasing the vulnerabilities of strategic civilian and military communications-information systems and command and command systems for forces involved in missions and operations in and outside Territory of the country. This requires adequate and timely development and acquisition of cyber defense capabilities as an integral part of the capabilities of protecting the national security management system related to defense and ensuring the territorial integrity of the Republic of Bulgaria, the support of international peace and security in alliance and coalition format And the contribution of the armed forces to national security in peacetime in dealing with crises of a non-military nature.

Cyber Security - a state definitely measured by the level of confidentiality, integrity, accessibility, authenticity and fault-tolerance of information resources, systems and services. Cyber security is based on effective building and maintenance of active and preventive measures. Cyber security usually means the precautions and actions that can be applied to protect cyber space, both in civil and military fields, from threats that are related to its independent networks and information infrastructure or may disrupt their work. The goal of cyber security is to preserve the availability and integrity of networks and infrastructure as well as the confidentiality of the information contained therein.

According to Anders Fogh Rasmussen, NATO Secretary General 2009–2014, "A cyber attack may put one country on its knees without a single soldier having to cross its border, and it is no exaggeration to say that cyber attacks have become a new form Of a constant low-level war". Cyber attacks are a direct threat to the security of citizens and the functioning of the state, economy, society, science and education. They can be done at a distance, with simple and effective mechanisms, minimal economic resources, and cause considerable damage with material and even human losses. Cyber attacks have no national, cultural or legal boundaries. Risks and threats in cyberspace are difficult to define because of the complexity of determining the source of the impact, the goals and motives, the rapid the escalation of the threat and the difficult predictable prospects for development, the complexity and intensity of modern communication and information processes, the dynamics of logical and physical connections and the uncertainty of processes. Cyber attacks are getting more and more and more serious. A national approach to addressing threats is designed to develop a response strategy based on pre--existing analyzes and assessments. Alongside cybersecurity, attention should be paid to physical security as well as measures to ensure the security of the virtual space. It is necessary to develop adequate policies and make real decisions about

tackling cyber crimes against critical infrastructure sites. Experts' predictions that the Internet security issue will grow in the era of the Internet is already coming true. However, in early awareness of the risk, taking the necessary precautions and assuming responsibility, the situation can be mastered. On the basis of the policies for critical infrastructure protection (CI) considered by cyber attacks, it can be concluded that there is no clear boundary between internal and external security due to their interdependence. On the other hand, IT management requires new strategies to address cyber threats based on improved methods and approaches.

When looking for a solution to cybersecurity, we need to address the need to protect cyber networks and create adequate policies to address cyber-attacks.

References:

Law on state agency for National Security. Закон за държавна агенция Национална сигурност.

Disaster and Accident Act – Закон за бедствия и аварии.

Velichka Milina „The new paradigm of energy security «Sofia 2013.

Величка Милина „ Новата парадигма на енергийна сигурност“ София 2013.