PROTECTION OF THE CRITICAL INFRASTRUCTURE – BEHAVIORAL ANALYSIS

Teodora Gechkova
Department National and Regional Security, UNWE, Bulgaria, tgechkova@unwe.bg
Tiana Kaleeva
Department National and Regional Security, UNWE, Bulgaria, tkaleeva@e-dnrs.or

Abstract: The report describes the importance of the critical infrastructure for the normal functioning of the societies. It is essential for the security, defense and wellbeing of the countries, as well as their political and economic life. The material offers a definition of critical infrastructure, the most commonly included sectors and components of it and the concept of a united critical infrastructure between numerous member states. Along that, different challenges for the critical infrastructures are presented:

- **Threats** – natural, human and technical/accidental;
- **Risks** – technological, economic, human-factor, terrorist attacks, criminal actions and cyber-security;
- **Vulnerable sectors** – energy, critical manufacturing, water systems, transportation systems, commercial facilities, chemical, food and agriculture.

The report outlines the positive influence of the behavioral analysis in preserving security and defense. It is especially important for overcoming the challenges critical infrastructure is facing. It is a provider of new technology and approach for maintaining security and promoting sustainability.

The UK government ***Project Servator*** is presented as an example of a good practice in this field. It is designed to be used by trained specialists in crowded places in detection of suspicious or hostile behavior and out of ordinary activities.

In addition to project Servator, an ***Action Counters Terrorism Awareness E-learning*** project is applied in UK aiming to encourage the citizens to pay attention, efficiently identify unusual behavior and promptly report it. It also provides information what actions should be undertaken in case of bomb threats or weapons attack.

Analogically, the USA Department of Homeland Security has implemented ***"If You See Something, Say Something"*** campaign. Its target is to raise awareness over the mass public through educational posters and brochures with specific information how to spot abnormal behavior.

Moreover, the report presents the ***NEC's Behavior Detection*** system as another good method of managing the security of crowded places which are part of the critical infrastructure. The program is an efficient instrument in spotting suspicious behavior and masked individuals, detecting intrusions to prohibited areas and identifying spaces with concentration of huge amount of people.

Keywords: Critical infrastructure, Security threats, Behavioral analysis, Protection programs

1. INTRODUCTION

In the contemporary world, the critical infrastructure is part of the everyday life of most of the developed and developing countries. It is vital for the functioning of the economic and political life of any given society and for the maintaining of the security and sustainability of the population. That is why preserving its normal existence and functioning is of fundamental importance. The critical infrastructure is exposed to countless of threats and risks that might cause vulnerability, disruption or destruction of its crucial sectors. That imposes the need of implementation of modern and innovative approaches and technologies for protection and support of the critical infrastructure as a whole.

2. CONCEPT OF THE CITICIAL INFRASTRUCTURE

In general terms the critical infrastructure could be defined as an element, system or parts of it, which are situated in a particular country and are of crucial importance for ensuring its vital public functions, as well as, maintenance of the safety, security, health, economic or social welfare of the citizens, and the destruction or impairment of which would lead to serious negative consequences in the country as a result of its inability to preserve their normal functioning.

Each country should define the components of its critical infrastructure based on its own needs, potential risks and threats and experience in this field. It should cover the strategic sectors with their objects, entities and operators in its territory, including the products and services manufactured as final output presented to the consumers. That is why the critical infrastructure usually covers sectors such as energy, transport, communication, finance, healthcare, education, defense, water and food resources, chemicals and others. As essentially important for the normal processes of each country, they are the most commonly included sectors among the different critical infrastructures around the world.

Although the separate countries have their own unique critical infrastructure, there are cases in which they might be a part of a united critical infrastructure. An example of that is the critical infrastructure of the European Union (EU). According to the European Council Directive 114/2008 the „European critical infrastructure (ECI) is defined as a critical infrastructure located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States" (European Council, Directive 114/2008). Each member state with potential ECI on its territory is obliged to enter in discussions with other member states which might also be affected by the ECI.

The Directive also stated that cross-cutting criteria should be applied in order to be estimated the significance of the impact in case of destruction of ECI. These criteria are: assessment of potential number of casualties; estimated economic effects in terms of economic loss or deterioration of the provided products and services; and assessment of the public effect regarding the public confidence and the disruption of the daily life of the population.

3. CHALLENGES FOR THE CRITICAL INFRASTRUCTURE

As vital providers of crucial products and services to the general public, the critical infrastructure sectors are exposed to numerous factors that might negatively affect them. Some of the most **vulnerable sectors** (or their derivatives) are energy, critical manufacturing, water systems, transportation systems, commercial facilities, chemical, food and agriculture (CIPSEC website, ICS/SCADA networks threats and defense).

The three main **threats** for the components of the critical infrastructure are based on **natural** factors (e.g. tsunamis, earthquakes, floods, hurricanes, fires, volcanic eruptions and others), **human** factors (such as theft, financial crimes, fraud, economic espionage, terrorist acts, rioting, product tampering, etc.) and **technical or accidental** factors (e.g. infrastructure and hazardous accidents, safety-systems failure, power-grid failures and others) (Tal, J., America's Critical Infrastructure: Threats, Vulnerabilities and Solutions).

The critical infrastructure in general is dealing with a wide range of **risks** – from **technological** (such as aging infrastructure elements, technological malfunction in the systems or inefficient devices), **economic** (e.g. as price volatility of commodities and final products and services, fluctuations in foreign currencies, challenges in the economic or political environment) and **human factor** (such as unqualified employees or lack of specialists in the particular field), to **terrorist attacks**, **criminal actions** and **cyber-security** risks. Possible cyber-security risks are external hacking, malware, social engineering, spam, insider data leakage/theft, denial of service, mobile device theft and physical security attacks (Federal Virtue Training Environment, Cybersecurity and Critical Infrastructure).

4. THE BEHAVIORAL ANALYSIS IN THE PROTECTION OF THE CRITICAL INFRASTRUCTURE

In its everyday activities the critical infrastructure is involving thousands of individuals, from the mass public that is using its goods or services to the specialists and staff working on its territory. As well as that, the infrastructure includes numerous types of specific devices, equipment and facilities which destruction would lead to disruption of the normal process of the given country. That is why proactive measures towards the prevention of negative impact on the components of the critical infrastructure are necessary. Furthermore, the protection of the individuals on the critical infrastructure's territory is of significant importance. The maintaining of stable and secured environment throughout the sectors of the critical infrastructure is crucial.

Along with the already implemented and available security measures and technologies, the introduction of behavioral analysis programs could influence positively the preservation of safety and facilitate the staff members in this process. More and more countries are searching solutions to the security challenges they are facing in the form of behavioral analysis which could transfer security beyond the traditional defense methods and instruments.

As an example of a good practice in this field is the United Kingdom's ***Project Servator***. It operates in crowded locations and uses behavioral detection. Its goal is to disrupt different criminal activities (together with terrorism) while including the mass public in the process through encouragement for reporting of suspicious acts and behavior.

The Servator Project uses specialists trained in identifying individuals with hostile intent and detect them before the criminal activity or terrorist attack occur. The project deploys different types of human resources – armed police officers, uniformed and plain clothes officers, police dogs, vehicle checkpoints, marine police units, CCTV and Automatic Number Plate Recognition (UK Government website, Ministry of Defense Police: Project Servator). The mass public is also encouraged to report for activities and behavior out of ordinary, to stay vigilant and contact to the respective responsible institution.

As suspicious individuals who should be reported are considered those who frequently travels but is not clear to which destination, have multiple passports with different names, looks at extremist materials or promote hateful views. Received unusual deliveries, buying of large amounts of chemicals, or acquisition of illegal firearms are also suspicious activities which are supposed to be reported (Counter Terrorism Policing, Report Suspicious Activities).

Project Servator is considered to be successful in gathering intelligence that assists the Counter Terrorism Units across the UK in detecting, investigating and preventing terrorist acts. "It has resulted in arrests for a multitude of offences and is responsible for removing firearms, knives and drugs from the streets" (Counter Terrorism Policing, Servator).

In addition to this project UK is introducing the ***Action Counters Terrorism (ACT) Awareness E-learning***. Its aim is to provide guidelines for the individuals and organizations in understanding and mitigating terrorism in relations to the specific threats the country is facing. The e-learning consists of different modules and covers topics such as how to recognize suspicious behavior and what actions to undertake; how to deal with a suspicious item; how to respond to bomb threats; and what actions to take in case of firearms or weapon attack (Action Counters Terrorism, Awareness E-learning).

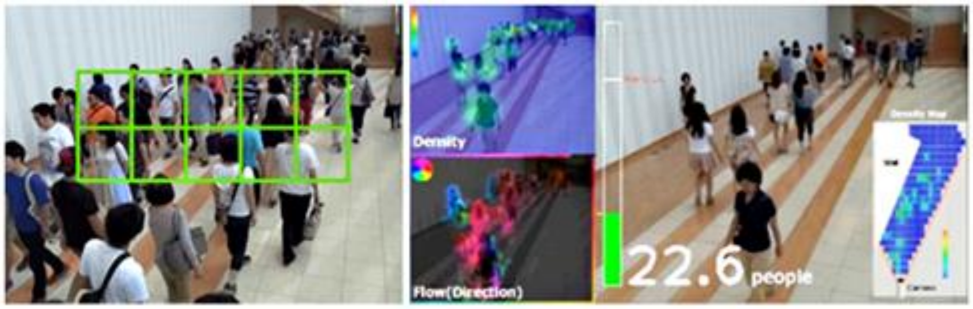
Along that, an App for smartphones or tablets concerning those topics is implemented. The app is an easily accessible information platform that provides potentially life-saving advices for actions that should be undertaken in an event of terrorist attack (ACT Awareness E-learning and ACT App).

Similar actions as those of the ACT Awareness E-learning are introduced by the United States Department of Homeland Security through the ***"If You See Something, Say Something"*** campaign. Its goal is to raise awareness among the mass public in detecting suspicious behavior. The campaign educates the citizens through posters and brochures which are the main indicators of terrorist-related crimes, how to pay attention to their surroundings and the importance of reporting activities that seems out of the ordinary (Homeland Security website, If You See Something, Say Something).

Another good practice is introduced by the Japanese ***NEC Corporation*** (Nippon Electric Company). The company is specialized in information technology and electronics, and promotes safety, security and efficiency. According to conducted tests by the US National Institute of Standards and Technology, NEC has developed the world's fastest and most accurate face recognition technology. The company is establishing a solution for assessment and support of the critical infrastructure through the usage of real-time surveillance, face recognition, video analytics and behavioral analysis for early detection of suspicious activities and detection of unwanted individuals (NEC website, Secure, visible and efficient critical infrastructure).

The integrated ***NEC's Behavior Detection*** improves the surveillance at the territory of the critical infrastructure without the need of operator to observe and analyze the video images and through that reduce the staff and equipment costs. The system is able to detect intrusions to prohibited areas, masked individuals and abandoned objects, as well as count the number of people and identify crowded spaces. The software is a convenient solution especially for the banking and financial sectors, stadiums, parking facilities, vehicle monitoring, airports, railway and metro stations and perimeter intrusions for critical infrastructures (NEC website, Behavioral Detection).

Fig. 1 NEC Behavioral Detection Interface



Analyzing people in groups
(green rectangle)

Detecting abnormal congestion, encircling
behavior and group evasion behavior

Source: www.nec.com

Besides the low costs, the Behavioral Detection System provides numerous additional benefits – spotting of moving individuals and objects in real time, early detection of abnormal behavior, easy defining of rules, possible scenarios and regions, alert notification. Last, but not least, there is no requirement for implementation of special hardware (NEC, Behavioral Detection Solution).

5. CONCLUSION

The critical infrastructure is a fundamental component of the modern and advanced world and as such its safety and security is one of the current top priorities. It is exposed to numerous factors that induce certain level of vulnerability to the strategic sectors of the critical infrastructure, along with different threats and risks. All that leads to the need of new programs and technologies for overcoming the challenges the critical infrastructure is facing nowadays and to promote safety, security and sustainability in the societies in general. The behavioral analysis could facilitate the process, offering innovative and timely approach toward the needs of the complex critical infrastructures.

ACKNOWLEDGEMENTS

This report is part of the university project ***"Improvement of the critical infrastructure security through the implementation of behavioral analysis"***, subsidized by the science and research fund of the **University of National and World Economy**.

REFERENCES

ACT Awareness E-learning and ACT App [Online]. Available at: https://www.highfieldelearning.com/act-awareness-e-learning-faqs (Accessed: 17 September 2021)

Action Counters Terrorism, Awareness E-learning [Online]. Available at: https://ct.highfieldelearning.com/index.php?mode=landing (Accessed: 20 September 2021)

CIPSEC website, ICS/SCADA networks threats and defense [Online]. Available at: https://www.cipsec.eu/content/icsscada-networks-threats-and-defenses (Accessed: 20 September 2021)

Counter Terrorism Policing website, Project Servator [Online]. Available at: https://www.counterterrorism.police.uk/servator/ (Accessed: 18 September 2021)

Counter Terrorism Policing website, Report Suspicious Activities [Online]. Available at: https://act.campaign.gov.uk/ (Accessed: 17 September 2021)

European Council, Directive 114/2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008.

Federal Virtue Training Environment website, Cybersecurity and Critical Infrastructure [Online]. Available at: https://fedvte.usalearning.gov/publiccourses/critical101/0060.htm (Accessed: 20 September 2021)

Homeland Security website, If You See Something, Say Something [Online]. Available at: https://www.dhs.gov/see-something-say-something/about-campaign/seesay-day (Accessed: 22 September 2021)

NEC official website, Critical infrastructure, Behavioral Analysis [Online]. Available at: https://www.nec.com/en/global/solutions/safety/criticalinfrastructure/behaviordetection.html (Accessed: 15 September 2021)

NEC official website, Secure, visible and efficient critical infrastructure [Online]. Available at: https://www.nec.com/en/global/solutions/safety/criticalinfrastructure/index.html (Accessed: 15 September 2021)

NEC official website, Advanced Image Analytics, Behavior Detection Solution Brochure [Online]. Available at: https://www.nec.com/en/global/solutions/safety/criticalinfrastructure/pdf/NEC_BDS_brochure_10082017_v3.pdf (Accessed: 15 September 2021)

NEC official website, Featured Technologies - Crowd Behavior Analysis [Online]. Available at: https://www.nec.com/en/global/rd/technologies/crowd/index.html (Accessed: 15 September 2021)

Tal, J., America's Critical Infrastructure: Threats, Vulnerabilities and Solutions (2018), [Online]. Available at: https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions (Accessed: 22 September 2021)

UK Government website, Ministry of Defense Police: Project Servator [Online]. Available at: https://www.gov.uk/guidance/ministry-of-defence-police-project-servator (Accessed: 20 September 2021)