Műszaki Katonai Közlöny

XXVII. évfolyam, 2018. 3. szám

Lilla Ronyecz[1]

CRITICAL INFRASTRUCTURE AND RESILIENCE

(A KRITIKUS INFRASTRUKTÚRA ÉS AZ ELLENÁLLÓKÉPESSÉG)

Resilience makes it possible to manage global challenges and risks in a more flexible way, which also facilitates continuous development. In this article the author first provides an overview of the key components of resilience and the most exigent questions regarding said components, then discusses international practices based on the experience of the past few years and the opinions of analysts and experts. After that, the focus shifts to the topic of resilience of essential systems and the extent of their vulnerability. Lastly, proposals are presented to increase the protection of critical infrastructure.

Keywords: *resilience, critical infrastructure, protection*

Az ellenálló képesség lehetővé teszi a globális kihívások és a kockázatok rugalmasabb kezelését a folyamatos fejlődés érdekében. A cikkben a szerző elsőként áttekinti a resilience legfontosabb elemeit, az egyes komponensek legégetőbb kérdéseit, majd számba veszi az elmúlt évek alapján a nemzetközi gyakorlatokat, valamint elemzők, szakértők véleményeit. Ezt követően a hangsúlyt a létfontosságú rendszerek ellenálló képességének kérdésköre kapja, tanulmányozza annak összetevőit, valamint sérülékenységének mértékét. Végezetül a szerző meghatározza javaslatait a kritikus infrastruktúrák ellenálló képességének növelésére.

Kulcsszavak*: ellenálló képesség, létfontosságú rendszerek, védelem*

RESILIENCE

Nowadays we face many complex challenges, which include hybrid warfare, mass migration, cyberattacks, the protection of critical infrastructure and maintaining the continuity of government – these factors constantly change the way threats should be addressed. In the face of these threats, it is of utmost importance to assess national resilience and to identify flaws. In the present study, I discuss the significance of resilience and examine its role in the operation of essential systems.

The concept of resilience (as NATO views it) became widely used after observing the type of hybrid warfare employed by Russia in Crimea and Ukraine. Apart from a military attack, member states might also suffer an economic, political or societal attack, thus it is important to assess national vulnerabilities and increase resilience. This is not a federal duty, but primarily a national and governmental one, which comprise a rather large area, which includes the protection of citizens and essential systems, cyberspace and armed self-defence. [1]

"The concept of resilience comes from the field of ecology, where it meant the adaptability of an ecosystem and its ability to survive in the face of change. " [2] This concept is widely used in other fields of science, but in the present study I examine it from the perspective of security

[1] PhD student at Doctoral School of Military Engineering NUPC,Ronyecz.Lilla@uni-nke.hu Orcid: 0000-0001-5062-5488

policy. "*According to NATO's official definition, resilience is the ability of societies and states to maintain their normal operation. As society (the population, but more importantly, economic operator) employs more and more modern technologies, it becomes increasingly vulnerable to external or internal attacks. The aim of these attacks is often the temporary disruption of normal operation instead of destruction. Globalisation and the advancement of science creates new dangers every year, so states must constantly improve their capabilities in order to keep up."* [2]

These definitions clearly show that resilience involves increasing the defences of society as a whole.

As the security situation in Northern Europe deteriorates, members of NATO and their partners increasingly become aware of the fact that Europe must face a number of challenges in terms of security, so preparing society for the hardships of armed conflict is inevitable. Increased efforts should be made to facilitate collaboration, joint action, deterrence and reinforcement, and each country should improve societal preparedness on a national level in order to create a new kind of security environment. As an example, apart from increasing military capabilities, Sweden also takes steps to increase the resilience of society as a response to declining security. In 2017, the government set up a Defence Commission, which aims to look beyond current security issues in order to establish the country's future defence policy. The Commission recently issued a report, which emphasizes that society must be prepared for the worst-case scenario, war. The approach adopted by Sweden is largely similar to the principal of resilience outlined in article 3 of the Treaty on which NATO is founded. Sweden collaborates with the Alliance in multiple areas, including the preparedness of citizens. [1] As part of the security strategy of the Alliance, resilience constitutes the measures taken by the classical military sphere in the following seven areas:

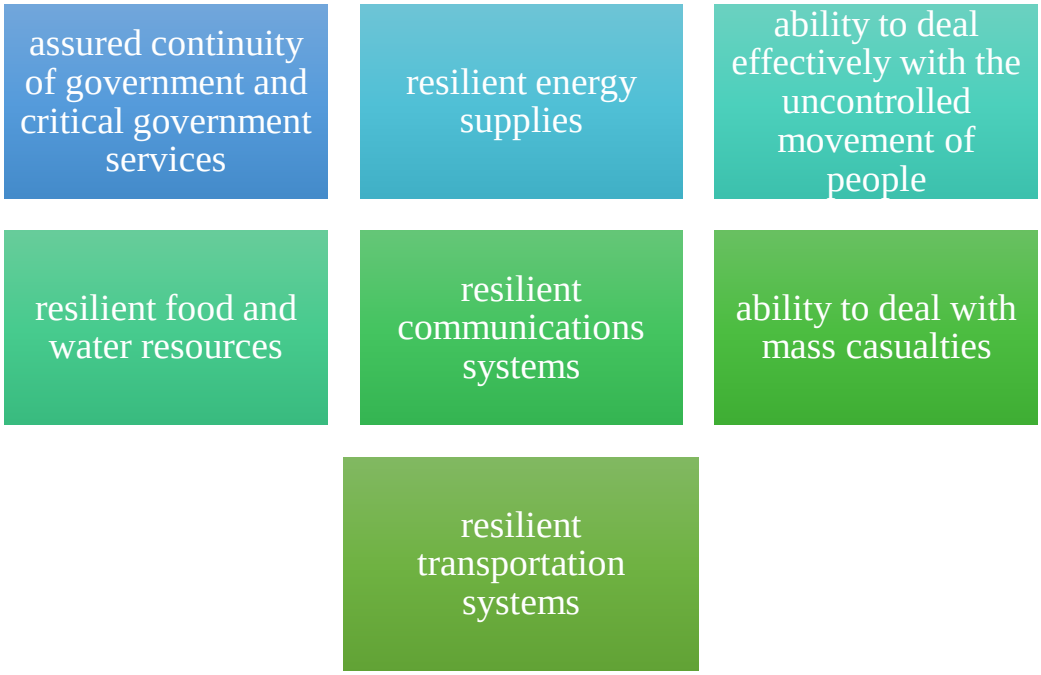


Figure 1: Groups of requirements that make up resilience [3]
Made by the author, 2018.

Based on these areas, it can be established that resilience is closely related to essential systems. In the case of sectors in Hungary, the continuity of government, energy supply, food and water resources and communication systems each belong to a separate sector, or constitute their own. It is important to bear this dichotomy in mind when analysing resilience and to complement defences accordingly.

Security policy experts claim resilience is not only about effective defences, but also the ability to quickly restore original conditions in case of an attack. [4]

According to the analysts at RAND[2], for the member states of NATO, resilience should primarily mean neutralizing Russian military, economic and political intimidation and pressure by reinforcing society at every level. [5] Some experts believe that maintaining good transatlantic relations between the US and its European allies is also a key component of resilience. [6] Other experts do not see hybrid warfare and the issue of resilience as newfound phenomena, as these merely represent an old problem that recently have resurfaced in a new form. [7] Some authors do not primarily discuss resilience in relation to the Russian threat, but in relation to extremist groups. Others, however, state that hybrid defence is only effective against adversaries who possess both conventional and unconventional assets. Terrorists do not fall into that category. [8] When it comes to resilience, it can also be observed that cyber security plays a very significant role within NATO. [2]

[2] RAND Corporation: Research and Development

Looking at expert opinions, it is clear that academic research conducted on the topic of resilience touch on many earlier academic debates. The protection of essential systems, cyber defence and the enhancement of military resilience are all individual areas, and the debate about resilience includes all of those. The question then arises as to how these separate areas can be coordinated in order to reinforce resilience on a societal level.

In the United States, increasing resilience is crucial for protecting civilians and essential systems, maintaining continuity of government, cyber defence and providing supplies for military forces.

The proposals suggest that these interdependent areas should be treated as a coherent whole. Coordination should be handled by a single, unified organization, otherwise the comprehensive perspective (that serves as the core of this concept) will not be attainable.

Resilience requires the interconnection of military and civilian spheres. This requires a governmental approach, which aims to synchronise the four interdependent areas. These four areas are the following: identifying key vulnerabilities and associated risks, coordinating interdepartmental decision-making regarding national and NATO planning processes, ensuring combat readiness of the military and preparedness of the civilian sphere, and expanding the available resources.

Now that I have provided an overview of resilience, I move on to give an accurate picture of the resilience of essential systems.

CRITICAL INFRASTRUCTURE RESILIENCE

It is important to distinguish between the protection of critical infrastructure and the resilience of critical infrastructure, as the two are not one and the same. A strategy study gives the following two definitions:

"Critical Infrastructure Protection (CIP) is the term used only to describe actions or measures undertaken to mitigate the specific threat of terrorism.

Critical Infrastructure Resilience (CIR) is the term used to describe an all-hazards approach to CI activities across the spectrum of prevention, preparedness, response and recovery." [9] While the protection of essential systems involves action and active measures, resilience of essential systems is about prevention, preparedness as part of a comprehensive approach.

Critical national infrastructures include eleven main sectors, which are necessary for everyday life. Threats to these sectors (either natural or human) could potentially make it impossible to maintain Hungary's general and economic security or public health. Technical innovation is necessary to address the security and resilience of essential systems.

Essential systems provide those basic services that society's everyday operation hinges on. Proactive and coordinated efforts have to be made to reinforce and maintain the security, operability and resilience of those critical infrastructures (assets, networks and systems) that are essential with respect to public trust and the protection of the country. Infrastructures are diverse and complex. They include distributed systems, different organizational structures and operating processes that are all interdependent functions and system in both the physical and cyber space.

Operators are in a unique position, as they have to manage the risks pertaining to individual operations and assets and define effective strategies to make systems more secure and resilient. Apart from being secure, essential systems should also be able to quickly react to threats and resist them. Following an incident, it is crucial that normal operation is restored as soon as possible. The following four elements depict the resilience of infrastructure.

Figure 2: Critical infrastructure resilience
Made by the author, 2018. [1]

Resistance means physical protection. The essential system is able to withstand the first shock of an attack and continue operation. Consider the resistance of electricity transponders to storms.

Reliability covers the sustainability of an infrastructure under different circumstances (e.g. extreme fluctuations in temperature). Redundancy is the adaptability of an asset or service, for example two physically separate water supplies for a critical facility. Response and recovery covers the reaction to threats and hazards, as well as quick recovery. These four elements represent the ways in which infrastructural resilience can be achieved. [1]

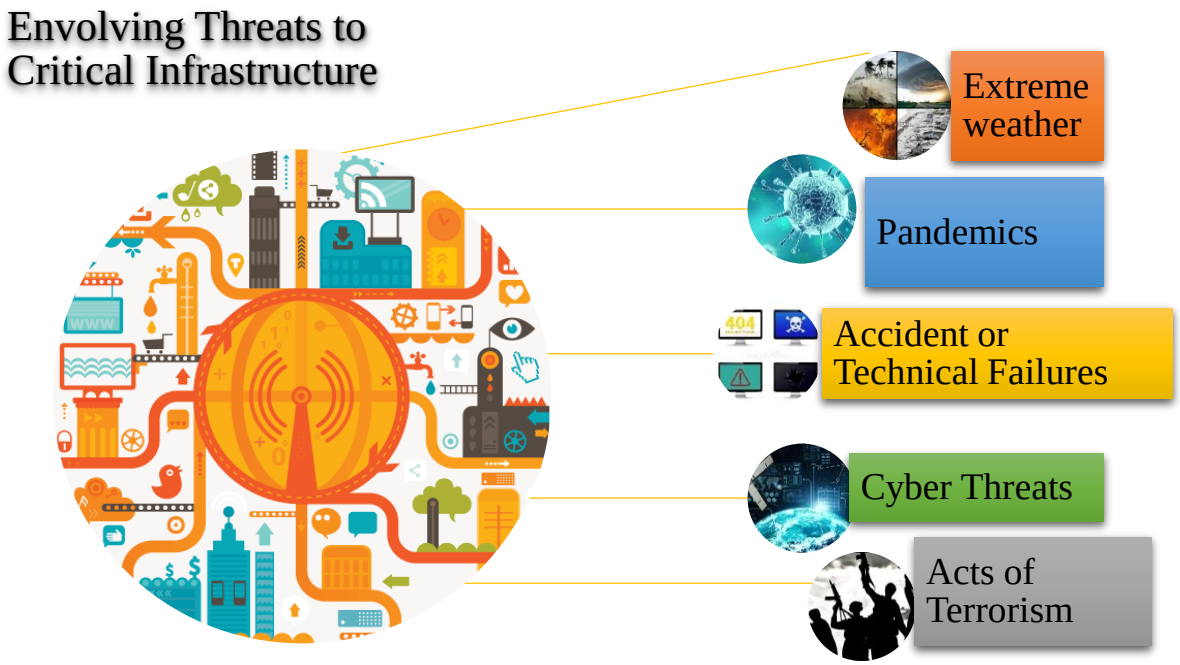
Governments have a hard time establishing proper security, as the expectations are unrealistic. Resilience requires that the findings of studies on comprehensive security conducted in the last few decades be put into practice simultaneously, so as to eliminate the vulnerabilities of society against a hybrid attack. This shows that the areas experts deem essential for reinforcing resilience are very diverse. Furthermore, the number of threats is rising and their nature is constantly changing.

It can be observed that cyber security is closely related to hybrid defence, so implementing proper cyber defences is crucial in increasing the resilience of society. In certain countries, the main element of effective hybrid warfare is the close cooperation of law enforcement agencies.

As an example, Lithuania's special forces can quickly be deployed anywhere in the country in case the police encounter a hostile armed group whose purpose, presumably, is to prepare a hybrid attack. Due to their flexibility and deployability, the importance of special task forces is increasing. The most serious future threats to essential systems and state security are cyberattacks. However, the most vulnerable targets are she so-called soft targets (e.g. the population) that are unable to resist threats or violent attacks.

Essential systems support the country's economy, society and national security. Interdependent infrastructures are increasingly global, complex and sensitive to disruptions. The concerned authorities must pay closer attention to mitigating the impact of potential disruption to essential systems, as well as their resilience. The current approaches to risk assessment and control often fail to consider some relevant connections, like the interdependence of certain sectors and the risk factors pertaining to cyber security. As a result, developing an integrated risk assessment plan and governance strategies that allow for proactive resilience remains a considerable challenge. [10] Achieving resilience and flexibility requires accurate information and risk analysis. Mitigating response and recovery activities contribute to the reinforcement of the resilience of critical infrastructure. Risk analysis ensures better security and flexibility. A risk is a potential incident, event or an undesirable outcome of an event that occurs as the result of probability[3] and associated consequences. Some infrastructures have been exposed to physical risks for a long time, but the growing number of natural disasters and the emergence of IT devices affect the operation of infrastructures in its entirety. This risk has had to be taken into account more emphatically throughout the years, as the number of cases of malicious damage in this area is increasing to this day. [11]

[3] Probability is based on the correlation between threats and vulnerabilities.



3. Figure 3: Evolving Threats to Critical Infrastructure [11]
Made by the author, 2018.

The above figure shows that the risk environment of essential systems is complex and uncertain. These threats, vulnerabilities and consequences emerged in the last 10 years, so a proper response has become necessary. As the first step I propose conducting a risk analysis that takes into account the new type of challenges.

SUMMARY

NATO and the European Union are increasingly committed to strengthen national resilience. However, NATO and the EU can only play a secondary role in improving the resilience of individual member states, therefore the different departments must seek each other's aid to facilitate collaboration.

All these lead to the conclusion that the comprehensive protection of the essential systems cannot be realized on a sectoral level, so it is crucial that local authorities cooperate in implementing and maintaining such protection. Furthermore, the resilience of critical infrastructure can only be further increased, if the state establishes a closer relationship with private enterprises.

Based on available data, the EU and NATO can get a coherent picture of risks and vulnerabilities present in each partner state. The data comes from diplomatic and intelligence networks, operating areas and sectoral and policy experts. Data shows that there are several overlapping risk analysis procedures, but there are also significant shortcomings regarding this area. These analyses often ignore local resilience, when in fact mitigation of vulnerabilities should first be adopted on a local level.

I find that it is necessary to develop a type of risk assessment that gives priority to new forms of challenges (like hybrid warfare), and in so doing allows for the implementation of risk management strategies that increase the resilience of essential constituents.

REFERENCES

[1] Dr. Björn von Sydow: Resilience: Planning for Sweden's "Total Defence" https://www.nato.int/docu/review/2018/Also-in-2018/resilience-planning-for-swedens-total-defence/EN/index.htm (date of download: 23/04/2018)

[2] NATO. (2016.). Resilience: a core element of collective defence. http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/ (date of download: 23/04/2018)

[3] Jamie Shea: Resilience: a core element of collective defence: https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

[4] Fassi, E., Lucarelli, S., & Marrone, A. (2015.). What NATO for What Threats - Warsaw and Beyond. Istituto Affari Internazionali: http://www.iai.it/sites/default/files/what-nato-for-what-threats.pdf (date of download: 23/04/2018)

[5] RAND. (2015.). NATO Needs a Comprehensive Strategy for Russia RAND: http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE143/RAND_PE143.pdf

(date of download: 23/04/2018)

[6] The Atlantic Council és CSIS. (2009.). Alliance Reborn: An Atlantic Compact for the 21st Century. Voltaire Network: http://www.voltairenet.org/IMG/pdf/Atlantic_Alliance_Reborn.pdf (date of download: 23/04/2018)

[7] Seely, R. (2015.). Russia's New Warfare Tools and the Link to Soviet Active Measures. Georgian Review: http://georgianreview.ge/wp-content/uploads/2015/09/bob-pdf.pdf (date of download: 23/04/2018)

[8] Aaronson, M., Diessen, S., Kermabon, Y. d., Long, M. B., & Miklaucic, M. (2011.). NATO Countering the Hybrid Threat. CIAO: https://www.ciaonet.org/attachments/19704/uploads (date of download: 23/04/2018)

[9] Officw of Emergency Management: NSW Critical infrastructure resilience strategy Discussion Paper September 2017. https://www.emergency.nsw.gov.au/Documents/publications/Discussion-papers/NSW-Critical-Infrastructure-Resilience-Strategy-Discussion-Paper.pdf (date of download: 23/04/2018)

[10] Official website of the Department of Homeland Security: Critical Infrastructure Design and Adaptive Resilient System https://www.dhs.gov/science-and-technology/csd-cidars (date of download: 20/04/2018)

[11] NIPP 2013. Partnering for Critical infrastructure Security and resilience https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf (date of download: 21/04/2018)