Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Andras Hugyik, *Connections QJ* 19, no. 4 (2020): 25-38
https://doi.org/10.11610/Connections.19.4.02

Research Article

Best Practices in the Application of the Concept of Resilience: Building Hybrid Warfare and Cybersecurity Capabilities in the Hungarian Defense Forces

Andras Hugyik

Abstract: In its Global Strategy for foreign and security policy, the EU applies resilience as a comprehensive concept of internal and external security. In parallel, at the 2016 Summit in Warsaw, Allied leaders decided to boost NATO's resilience to the full spectrum of threats. Each NATO member needs to be resilient to a major shock caused by a natural disaster, failure of critical infrastructure, a hybrid, or an armed attack. Hybrid warfare, including cyberattacks, is recognized as a significant security challenge.

The National Security Strategy of Hungary, adopted in 2020, confirms that the primary international framework of Hungary's security and defense policy is NATO and EU membership and highlights the need to enhance the country's resilience against hybrid attacks. This article provides an analysis of the application of the concept of resilience in the Hungarian defense sector. It introduces the development of the resilience of the Hungarian Defense Forces against hybrid threats, including their cyber component, while generating options for the decision-makers regarding the military and information instruments of national power. The author identifies potential hybrid threats against Hungary, a possible cyberattack scenario, and lines of effort to achieve a feasible level of resilience to such threats. He takes account of the political and military environment, as well as wider national issues in view of hybrid threats and main features and dilemmas of cyber warfare, thus aiming to facilitate the application of the concept of resilience in Hungary.

Keywords: resilience, security policy, military, intelligence, hybrid warfare, cyber defense, EU, NATO, Hungary.

Introduction: Applying the Concept of Resilience in Hungary

The purpose of applying the concept of resilience is to strengthen the abilities of systems, organizations, policies, and individuals to respond well to external impacts. Many experts agree that "the recent enthusiasm for the concept of resilience across a range of policy literature is the consequence of its fit with neoliberal discourse. This is not to say that the idea of resilience is reducible to neoliberal policy and governance, but it does fit neatly with what it is trying to say and do."[1]

The ideology of neoliberalism primarily sees the guarantee of economic growth, welfare, liberty, and the common good in the 'liberalization' of markets. The neoliberal state radically departs from the redistribution of the welfare state, takes business- and market-friendly measures to protect private equity gain, and turns citizens into entrepreneurs and consumers.

The collapse of neoliberal hegemony after 2008 has led to a new wave of populism. Populist parties and movements include both left- and right-wing actors. One of their few common characteristics is that they all criticize the ruling elite and its ideology, claiming that the people are oppressed by the elites.

According to the left-wing rhetoric, the social and economic policy of Orbán's populist government in Hungary is strengthening the nation's capitalist class, selling out cheap workforce for foreign industrial investors while disciplining those workers, and performing centralized control of the poor, primarily living in rural areas. The purpose of its cultural policy is to promote the official Hungarian ideology of the era before 1938; a conservative, Christian, nationalist ideology with historical lies, an unjust social system, hateful atmosphere, and the hidden intention to recover territories lost after World War I. Orbán perceives the neoliberal European Union, the international capitalists' secret fraudulent practices represented by George Soros, and migrants as enemies to declare his political opponents as the enemy of the nation and to take the role of the rescuer of the nation.

While the government is attacking some of the EU's values in front of the political audience and is confronted loudly, in terms of economic processes, it is a subordinated ally of European capitalists.[2] Due to constructivist elements of Viktor Orbán's regime-building politics,[3] democracy, the rule of law, and plural-

---

[1] Jonathan Joseph, "Resilience as Embedded Neoliberalism: A Governmentality Approach," *International Policies, Practices and Discourses* 1, no. 1 (2013): 38-52, https://doi.org/10.1080/21693293.2013.765741.

[2] Tamás Gerőcs and Csaba Jelinek, "The System of Hungarian National Cooperation in the Context of the European Union – on Hungary's EU Integration in a Historical Sociological Approach," *Analízis* (2018): 12-33, quote on p. 23, www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek_nemzeti_2018.pdf, – in Hungarian.

[3] Gábor Illés, András Körösényi, and Rudolf Metz, "Broadening the Limits of Reconstructive Leadership - Constructivist Elements of Viktor Orbán's Regime-building Politics,"

ism in Hungary have become limited and resulted in the establishment of a country with illiberal democracy. In Hungary, those in power suggest that leftists and liberals are not part of the nation, and all that is left or liberal, be it the person, any artwork, or just a point of view or an approach, should be deemed as alien and should be rejected because that goes against the official national Christian conservative course.

Perhaps this political climate also contributes to the fact that in Hungary, only NATO-related defense sciences initiate develops of resilience-based security and law enforcement concepts. However, a more plausible explanation is that, as opposed to the generally accepted, comprehensive security policy and crisis management approach, in the case of resilience, we should focus on national-level solutions. Many Hungarian experts regard this as evidence of the appropriateness of the efforts to develop a comprehensive approach at the national level, which was launched in our country in 2010.

The majority of Hungarian security policy experts consider that in 2014, during the Ukrainian crisis, both NATO and the EU found the adequate response to hybrid threats in increasing nations' resilience and in supporting military efforts with civilian tools (civil preparedness). The very essence of this solution lies in the coordinated application of military and civilian crisis management components, which is also a basic principle of the comprehensive approach.

Therefore, it can be established that the background, the fundamental principles, and the toolset applied for resilience and civil preparedness are practically the same as the comprehensive approach itself; they are a mere re-interpretation thereof in a different context. Thus, resilience and civil preparedness did not bring about a different mindset or a set of requirements; yet, these cannot be regarded as identical to any already existing sets of tasks under any legislation.

Therefore, it is necessary to statutorily appoint a national coordinator for the purpose of both resilience and civil preparedness and to define the scope of national-level tasks, the bodies and the organizations responsible for their implementation, the cooperating organizations, and the procedural rules of cooperation. Given that the task requires close and comprehensive cooperation throughout the government, the effective implementation should fall within the competence and capabilities of the system of defense administration.[4]

The British Journal of Politics and International Relations 20, no. 3 (2018): 790-808, https://doi.org/10.1177/1369148118775043.

[4] László Keszely, "Hybrid Warfare and National Resilience, or a Comprehensive Approach Reloaded," *Katonai Jogi és Hadijogi Szemle [Military Law and Military Law Review]* 1 (2018): 29-62, quote on 61-62, – in Hungarian, http://epa.uz.ua/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_029-062.pdf.

Building Hybrid and Cyber Warfare Resilience Capabilities in the Hungarian Defense Forces

Introduction of the Hungarian Defence Forces

The Hungarian Defense Forces (HDF) is the national defense force of Hungary. Since 2007, the Hungarian Armed Forces is under a unified command structure. The Ministry of Defense maintains the political and civil control over the army. A subordinate Joint Forces Command is coordinating and commanding the HDF units.

The armed forces have 28,000 personnel on active duty. In 2019, military spending was 1.904 billion USD, or about 1.2 % of the country's GDP, well below the NATO target of 2 %. In 2016, the government adopted a resolution in which it pledged to increase defense spending to 2 % of GDP and the number of active personnel to 37,650 by 2026. Military service is voluntary, though conscription may occur in wartime.

According to the Hungarian Constitution, the three pillars of the nation's security are the strength of the HDF, the system of the Alliance, and the citizens.

In February 2017, the Ministry of Defence disclosed the Zrínyi 2026 development program, which intends to increase the capability of active armed forces, the manpower of reserve forces, the military communication and information system, and cyber defense. These measures seem to be adequate steps for building resilience to hybrid threats.

Approach to Improve Resilience to Hybrid Attacks

Hybrid warfare denotes "the use of military and non-military tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure."[5] In other words, hybrid attacks combine military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, and deployment of irregular armed groups, and use of regular forces. Nowadays, hybrid warfare is considered a significant security challenge; within this wider threat category are cyberattacks that are perceived as one of the main threats to the modern society for every country.

Figure 1 illustrates a project for the Hungarian Defence Forces in the field of resilience development against hybrid attacks based on the findings of Adrian

[5] James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, quote on p. 76, https://doi.org/10.11610/Connections.15.2.06.

Feher.[6] Feher followed the steps of Army Design Methodology,[7] and hence describes the desired environment, defines the problem, and recommends an operational approach. Following a modification by this author, the project approach consists of six objectives, seven outcomes, and 15 proposed outputs in order to enhance the level of resilience against hybrid threats and thus protect the country. The figure aligns instruments of national power to each outcome.

The underlying logic of the proposed approach is that Hungary needs a hybrid defense strategy to combat potential hybrid threats. The military instrument of national power has to extend its impact and facilitate the improvement of information power, the development of information deterrence capacity to protect Hungary's sovereignty through citizenry's involvement. At the same time, there is a need for support from other agencies in establishing an informational deterrence capability to protect the population against hostile propaganda and cyberattacks. Since the military instrument is highly dependent on other instruments of national power, HDF must maintain and improve the collaboration with other stakeholders to establish a "whole-of-government" approach. The domain of information and the associated information operations play an important role in hybrid warfare. Historically, military operations have primarily focused on the enemy's capabilities and only secondarily on the weakening of its determination, while information operations target determination and willpower.

The aim of information operations is to achieve leadership supremacy, information domination, and information supremacy by employing psychological operations and operations on operational security, military deception, physical destruction, electronic warfare, public information, computer network warfare, and civil-military cooperation while using military information systems and intelligence information.[8] In the information operations doctrine currently applied by the Hungarian Defense Forces, the details of the concept of information operations have not yet been developed. The elements of information operations only partially reflect the activities and capabilities to be achieved in the information environment. Experts argue that the main challenge faced by the Hungarian Defense Forces is to attain the ability to address complex information issues: to quickly obtain, process, and integrate information into the decision-making cycle and to control the narratives of conflicts in the information space.

---

[6] Adrian Feher, "Hungary's Alternative to Counter Hybrid Warfare," Thesis (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 2017), 128, 123, https://apps.dtic.mil/dtic/tr/fulltext/u2/1038681.pdf.

[7] Headquarters, Department of the Army, *Army Design Methodology*, ATP 5-0.1, July 1, 2015, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_0x1.pdf.

[8] Zsolt Haig, "Methodology for Defining Critical Information Infrastructures, Information Warfare," ENO Advisory Ltd., August 1, 2009, p. 88, https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; Zsolt Haig and István Várhegyi, "Interpretation of Cyberspace and Cyber Warfare," *Military Science* (2008): 5-10, in Hungarian, http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf.

Project aim: **Protect the Sovereignty and Independence of Hungary by Enhancing Resilience to Hybrid Threats**		
Objectives	Outcomes and Instruments	Outputs
Possess a military deterrent capability to stop the enemy and support the intervention of NATO forces in Hungary	Increase the capability of volunteer conventional reserve forces **(M&I)** and establish volunteer unconventional reserve forces **(M&I)**	1, 2, 3, 4, **5**, 7, 9, 10, 12, 13, 14, 15
Maintain constitutional order and support the central government	Establish volunteer civil preparedness capability (M&**I**)	1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 14, 15
	Achieve commitment of the citizenry to the nation's defense **(I)**	1, 2, 3, 4, **5**, 7, 8, 9, 10, 12, 15
Assist NATO allies under collective defense condition	Increase active-duty forces' expeditionary capability (M)	1, 2, 3, **5,** 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Develop information deterrence capacity	Protect citizenry against hostile influence warfare and national power against cyberattack **(I)**	1, 2, 3, **5**, 6, 7, 9, 10, 13, 15
Prevent surprise	Build Integrated Intelligence, Surveillance and Reconnaissance – Provide operational security **(I)**	2, 3, **5,** 6, 9, 15
Follow "Whole-of-government" approach in defense	Provide for interagency cooperation **(DIME)**	1, 2, 3, 4, **5**, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Outputs: (1) Increase patriotism via social and traditional media; (2) Cease false sense of security; (3) Reveal and refute false news; (4) Recruit volunteers; **(5) Increase cyber warfare capability**; (6) Improve counterintelligence to identify and detect warning signals; (7) Conduct joint and combined rehearsals (exercises); (8) Eliminate/ integrate extreme groups and establish the resistance movement; (9) Identify vulnerabilities and capability gaps; (10) Establish decentralized command and control with secure communications; (11) Enable quick response through the legal system; (12) Establish a system for readiness and mobilization; (13) Provide training and equip forces; (14) Build prepositioned stocks; (15) Ensure coordination of decision makers.		

Figure 1: Project to Improve Resilience to Hybrid Attacks.
Abbreviations: DIME – instruments of Diplomacy, Information, Military and Economy; M (Military Instrument), I (Information Instrument), M&I (Military and Information Instrument).

At the same time, the operational cyberspace capabilities of HDF should be developed, and their integration into both military planning and operation implementation should be established. To that end, the Hungarian Defense Forces must adopt a new mindset primarily focusing not only on the execution of combat activities but also on the desirable outcomes of such military operations, including the impact of such outcomes. In military doctrine, a broader interpretation of the information tool system is necessary. Treating it as a mere supporting function will not suffice.

Cyber Defense in Hungary

The Main Aspects and Dilemmas of Cyber Warfare

Generally, in cyber warfare, states launch their operations for intelligence purposes with disruptive or destructive intentions and do so directly or through the involvement of third parties, such as hackers. Attacks may target critical public infrastructures, specifically the IT, information and communication systems used in the defense sector. In addition, hostile activities using social media and Internet platforms to influence civil society are increasingly common. In a broader sense, cyber warfare covers all attacks realized in cyberspace with a useable result for the attacker in military or political terms.[9] Experience has shown that a cyberattack only imposes a substantial burden on a country if it is coordinated (relates military control with a strategic goal, to which each operational activity is subordinated), comes in waves (types and targets of attacks are diverse, unpredictable and consecutive), is multi-sectorial (affects several industries, while defense coordination generally covers only a small scope of industries), is supported by information acquired by intelligence (information required for attacks is not only from open sources but also from intelligence collection and analysis) and is primarily realized to cause damage to the enemy. The aim is to make the country and its citizens feel the attack, i.e., such attacks must be very obvious and must involve emotional impacts –characteristics that set them apart from cyber espionage.[10] Cyberattacks are generally not used by states for destructive purposes in peace periods, as remaining in the "gray zone" between peace and war serves their best interests. This does not mean that they would not be able to go beyond this zone if necessary.

---

[9] Tibor Rózsa, "Theory, Practice and Tendencies of Information Operations," *Defence Review* 5 (2019): 82-84; Gábor Berk, "Cyberspace, Its Dangers and the Current Situation of Cyber Defense in Hungary," *National Security Review* 3 (2018): 5-21, http://epa.oszk.hu/02500/02538/00024/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_03_005-021.pdf; Zsolt Csutak, "New Warfare of New Times – Cognitive Security in the Age of Information and Cyber Warfare," *Defence Review* 5 (2018): 33-45, http://real.mtak.hu/84099/1/hsz_2018_5_beliv_033_045.pdf. – all sources in Hungarian.

[10] Csaba Krasznay, "Protecting Citizens in a Cyber Conflict," *Military Engineer* 7, no. 4 (December 2012), 142-151, quote on p. 144, http://hadmernok.hu/2012_4_krasznay.pdf.

The main dilemma of cyber warfare is the missing international regulation for cyberspace. Although the majority of UN Member States recognize the extension of the scope of international agreements for cyberspace, their applicability is still problematic.[11] This is because there is no internationally accepted definition of what we call a cyberattack or a cyber weapon. In addition, in a cyberattack, there is usually no clear declaration of war, attackers remain hidden in cyberspace, and the impacts to be expected also remain unassessed. Therefore, serious attention is paid to the application of relevant conventions to cyberspace operations.[12]

The Paris Call for Trust and Security in Cyberspace Initiative[13] was set up to guarantee secure cyberspace on the international level. Hungary joined the initiative, but the largest cyber-arsenal owners (the United States, Israel, Iran, China, Great Britain, or Russia) did not consider this necessary.

NATO's Cyber Defense

Combating cyberattacks is a priority for NATO. However, regarding the commonly used terms of cyberwar or cyberattack, it should be noted that there is no agreed definition of cyberwar or cyberattack in NATO's official terminology, and examples of definitions can only be found at the level of member states.

This is mainly due to the limitless nature of cyberspace and the constant expansion of the range of attack types it accommodates, but also to the interests of the Alliance. NATO does not deem the definition of cyberattack necessary because it individually evaluates simultaneous but different types of attacks to decide upon the nature of the alliance-level response.

Since 2007, NATO has been paying particular attention to cyber defense and cyber warfare. In 2012, the cyber defense was included in the Alliance's defense planning, and NATO's cyber defense guidelines were adopted at the 2014 Wales Summit. In Wales, the Alliance declared that it recognizes the validity of international law in cyberspace and included cyber defense among NATO's collective defense tasks.[14]

In 2016, in the communiqué of the Warsaw Summit, allies extended the area of operational warfare traditionally covering sea, air, and land to include cyber-

[11] "Trends in International Law for Cyberspace," NATO Cooperative Cyber Defense Centre of Excellence, May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf.

[12] David P. Fidler, "The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions than Answers," Council of Foreign Relations, March 15, 2018, www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

[13] Ministry for Europe and Foreign Affairs, "Cyber Security: Paris Call of 12 November 2018 for Trust and Security in the Cyber Space," *France Diplomacy*, www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[14] "Wales Summit Declaration," *NATO e-Library*, September 5, 2014, articles 72 and 73, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

space [15] and declared that a cyberattack against a member state could be considered by the Alliance as an attack on NATO as a whole and, if necessary, they may take collective measures in response.

In Warsaw, the Cyber Defense Pledge was adopted, wherein member states undertook a significant and rapid development of the protection of their national networks and infrastructures in line with Article 3 of the Washington Treaty, development of comprehensive cyber defense capabilities, and strengthening the cooperation in identifying and understanding threats while enhancing cybersecurity education and training. An important step in the development of NATO's cyber defense capabilities is the establishment of the Cyber Operational Center (CyOC) to coordinate the Alliance cyber operations within the Supreme Headquarters Allied Powers, Europe (SHAPE), starting in 2018.

In its cyber capabilities, NATO distinguishes passive and active defense capabilities: the former consists mainly of preventive, incident management, data and system restoration capabilities within its own network range. The latter is a capability of an offensive nature to deter and eliminate threats beyond the scope of its own networks.[16]

Cybersecurity within the Hungarian Defense Forces

In Hungary, defense against cyber threats and the definition of cyberspace as a theater of war appeared in strategic documents as early as 2012. In 2018, cyberspace as an autonomous theater of operation was incorporated in the Hungarian legislation (Section 80 of Act CXIII of 2011). The directions and modalities of the development of Hungarian military cyber capabilities are set out in the National Military Strategy (2012), the National Cybersecurity Strategy (2013), the Cybersecurity Concept of the Hungarian Defense Forces (2013), the above Warsaw Commitments, and the Zrínyi Development Program until 2026.

The National Military Strategy has identified "the creation of opportunities for network-based warfare" as one of the main goals to be attained by the Hungarian Defense Forces. On the one hand, computer-network warfare is aimed at influencing, degrading, and making impossible the operation of the opposing party's networked IT systems and, on the other hand, it seeks to maintain the operation of our own similar systems.[17] The timeline of building these cyber ca-

[15] "Warsaw Summit Communiqué," *NATO e-Library*, March 29, 2017, articles 70 and 71, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[16] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence," NATO Parliamentary Assembly, April 18, 2019, pp. 4-6, www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf.

[17] According to Haig and Várhegyi, "Computer-network warfare includes the following activities: mapping the structure of computer networks; exploring hierarchical and operational features based on their traffic characteristics; registration of the content of the data flow on the network; deceptive, disruptive activity in networks; change

pabilities was defined in the Hungarian Defense Forces' Cybersecurity Concept. In this document, the initial level of cybersecurity capabilities had to be reached until 2014, the basic level cybersecurity capabilities between 2014 and 2016, and the full cybersecurity capabilities – after 2016. The concept aims, *inter alia*, to protect vital information system components, reduce their vulnerability, and eliminate potential damages as soon as possible.

Cybersecurity developments brought forth by the Hungarian Defense Forces form an integral part of the defense policy program. The HDF Electronic Incident Management Center was established in the framework of this program. In addition, further organizational and functional changes may be needed in the Hungarian Defense Forces to create a unified cybersecurity system. To that end, the type of cybersecurity organizations for the individual command levels should also be clarified. The main challenge in cybersecurity is to reduce response times and to enhance the efficiency of intelligence.

As of today, the majority of cybersecurity tasks of the Hungarian Defense Forces are performed by the Military National Security Service (MNSS). In recent years, in the implementation of MoD Instruction No. 85/2014, MNSS invested in the development of intelligence capabilities and capabilities, enabling the management of cyber incidents.

At a parliamentary hearing in 2019, the Chief of General Staff indicated that it had been foreseen to develop the cyber capabilities (non-existent at the time) in the near future. In 2020, the Government specified the areas within the Hungarian Defense Forces' cyber capabilities and operations that need to be applied or developed, and the Parliament added to the National Defense Act special rules regarding the military operations in cyberspace.[18]

Although the details are not entirely public, the 2020 defense budget shows that the cyber development of the military is a priority.

A Scenario of a Hybrid Attack against Hungary

It goes without saying that significant progress has been made at the national level in the field of cyber defense and security over the last ten years. However, we remain relatively defenseless and vulnerable to a well-structured, coordinated series of cyberattacks. According to Feher, these attacks can lead to

> the enemy's most dangerous course of action when the aggressor conducts full-spectrum hybrid operations, and it is able to procure enough supporters to fight against the central power, thus keeping the conflict under Article 5 threshold. With covert support from Special Operation Forces and conventional forces, the enemy can achieve fundamental surprise, paralyze the command and control system, successfully fight against Hungarian security forces,

and destruction of the program and data content of the target objects, and issues of protection against similar activities of the opposing party."

[18] Prime Minister's Office, *T/8029th Bill proposal* (12 November 2019), 5, 21-22, https://www.parlament.hu/irom41/08029/08029.pdf.

and establish functional alternative political power in occupied territories. In this situation, Hungary has to struggle without official NATO assistance in occupied or unoccupied lands.[19]

Based on this assumption and the thesis of Dr. László Kovács and Dr. Csaba Krasznay on a cyberattack scenario against Hungary,[20] I would like to present an escalation process that is completely conceivable today (Figure 2).

Findings

On December 10, 2019, the European Council adopted conclusions that set priorities and guidelines for EU cooperation to counter hybrid threats and enhance resilience to these threats. The conclusions call for a comprehensive approach to counter hybrid threats, working across all relevant policy sectors in a more strategic, coordinated, and coherent way.

In the case of Hungary, control over DIME, supportive and involved population, adequate military strength, effective intelligence and counterintelligence, and improved cyber resilience seem to be the relevant priorities, where resilience is defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption… [and] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[21]

Cyber resilience is the ability of an actor to resist, respond, and recover from cyber incidents to ensure the actor's operational continuity.[22] Strategic cyberattacks could target the nation's critical infrastructure and utilities, whilst operational cyberattacks are against the adversary's military.

At the same time, a cyberattack is a type of information operations within the information warfare aiming to "corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity, and availability of one's own information."[23]

The power in the information domain is vital for the nation to prepare the citizens for the negative influence of the enemy, keep or recover interactions

---

[19] Feher, "Hungary's Alternative to Counter Hybrid Warfare."

[20] László Kovács and Csaba Krasznay, "Digital Mohács: A Cyberattack Scenario against Hungary," *Nation and Security* 44 (February 2010): 44-56, in Hungarian, http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf.

[21] "Resilience," Glossary, NIST Information Technology Laboratory, Computer Security Resource Center (source: NIST SP 800-53 Rev. 4), https://csrc.nist.gov/glossary/term/resilience.

[22] Kjell Hausken, "Cyber Resilience in Firms, Organizations and Societies," *Internet of Things* (2020), 100204, https://doi.org/10.1016/j.iot.2020.100204.

[23] Anil Chopra, "Cyber Warfare a Key Element of Multi Domain Wars – Time to Push India," *Air Power Asia*, June 3, 2020, https://airpowerasia.com/2020/06/03/cyber-warfare-a-key-element-of-multi-domain-wars-time-to-push-india/

I.	Cyberattack (the first phase of a possible hybrid attack is a cyberattack)
I.1. Psychological operations	1. Intimidation: News about the alleged weakness of Hungarian cyber defense appears on a blog supported by a foreign secret service. 2. Distribution: The news that appeared on the blog are disseminated on social media, reaching tens of thousands of users. 3. Sharing: Due to sharing through pseudo-profiles created by foreign intelligence services, the news appears in more news flow and is spread further. 4. Highlighting: Due to the large number of sharing, the tabloid press also starts to cover the topic, and soon it becomes a topic in respected media as well.
I.2. Spectacular attacks	1. Overload attacks are launched against certain government websites, making some services unavailable for hours. 2. Some municipal and support agencies' websites are hacked, and messages threatening Hungary appear on their home pages. 3. Databases containing the personal data of tens of thousands of Hungarian citizens appear on the Internet.
I.3. Influencing politics	1. In a Wikileaks-type leak, government emails are published under the title HunLeaks; the international press begins to analyze them. 2. The "Hungarian Snowden" hands over classified documents to an investigative journalist. They are being analyzed by an international team of journalists. 3. An investigation ordered as a result of previous attacks finds sophisticated malware at the IT system of a public service provider. The purpose of malware is to obtain data. According to the report on the investigation, the malware has been running for at least two years.
I.4. Infrastructure attacks	1. Attacks on telecommunications: Most telecommunication services become inaccessible. Government communication is also hampered. Defense coordination slows down and is blocked. 2. Attacks on the finance system: Online banking is paused; international financial transactions are also suspended. 3. Attacks on electricity services and transport: District level power outages occur; transport is paralyzed.
II. Aggressor conducts full - spectrum hybrid operations	The aggressor conducts a combination of special and conventional military operations, uses intelligence agents, political provocateurs, media influence, economic intimidation, proxies and surrogates, paramilitaries, terrorists, and criminal elements. The aggressor can achieve a fundamental surprise, paralyze the command and control system, successfully fight against Hungarian defense and security forces, and establish functional alternative

	political power in occupied territories. In this situation, Hungary has to struggle without official NATO assistance in occupied or unoccupied lands.

	Resilience development at the national level	Resilience development at HDF level
I. Hybrid attack	Designate a national coordinator for resilience and civic preparedness, define the national tasks, bodies, and organizations responsible for and cooperating in their implementation, and procedures for cooperation. Defense administration seems to be the right system to ensure full-spectrum government cooperation.	Implement the proposed project (Figure 1) in order to achieve the desired aim (end-state), to protect the country by improving resilience against hybrid attacks. The figure aligns instruments of national power to each outcome.
II. Cyberattack	Raising information security awareness in society, strengthening cyber defense organizations, creating alternative, emergency infrastructures, strengthening the toolbox for coordinated, centralized cyber defense, strengthening partnerships between the administrative, business, and scientific spheres.	The main task of HDF is to deal with information challenges in a complex way: both to quickly obtain and process information and integrate it into the decision-making cycle, and to control the narratives of conflict in the information space. The operational capabilities in cyberspace and their integration into military planning and execution need to be established.

Figure 2: Possible Hybrid Attack against Hungary and Provision of Resilience.

between the state and the people, and terminate the citizens' false sense of security.

On the basis of NATO's interpretation, resilience at the national level is the combination of civilian preparedness and military capability.[24] This means that we should address the following challenges: raising information security aware-

[24] Gustav Pétursson, "NATO's Policy on Civil Resilience: Added Value for Small States?" SCANSE Research Project, Policy brief no. 5 (26 June 2018): 2, http://ams.hi.is/wp-content/uploads/2018/06/NATO%C2%B4s-Policy-on-Civil-Resilience-Added-Value-for-Small-States.pdf.

ness in society; strengthening cyber defense organizations, creating alternative, emergency infrastructures (elements); strengthening the toolbox for coordinated, centralized defense; strengthening partnerships between the administrative, business and scientific spheres; improving the resilience of HDF against hybrid warfare, including cyberattacks, by the execution of the proposals in this article.

To establish resilience against cyber threats, the HDF should be able to deal with information challenges in a complex way: both to quickly obtain and process information and integrate it into the decision cycle, and to control the narratives on the conflict in the information space.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 19, 2020 is supported by the United States government.

About the Author

Andras **Hugyik**, PhD in military science, is a retired police colonel, a chief councilor of the Hungarian police. He is an engineer, economist, and political expert. He is a former adviser to GUAM, OSCE, EUBAM, and UN – OPCW Joint Investigation Mechanism. Before joining these international organizations, he served in the Military Intelligence, the internal security service of the Hungarian law enforcement agencies, and the counter-terrorism center of Hungary.
E-mail: seniorhugyik@gmail.com.