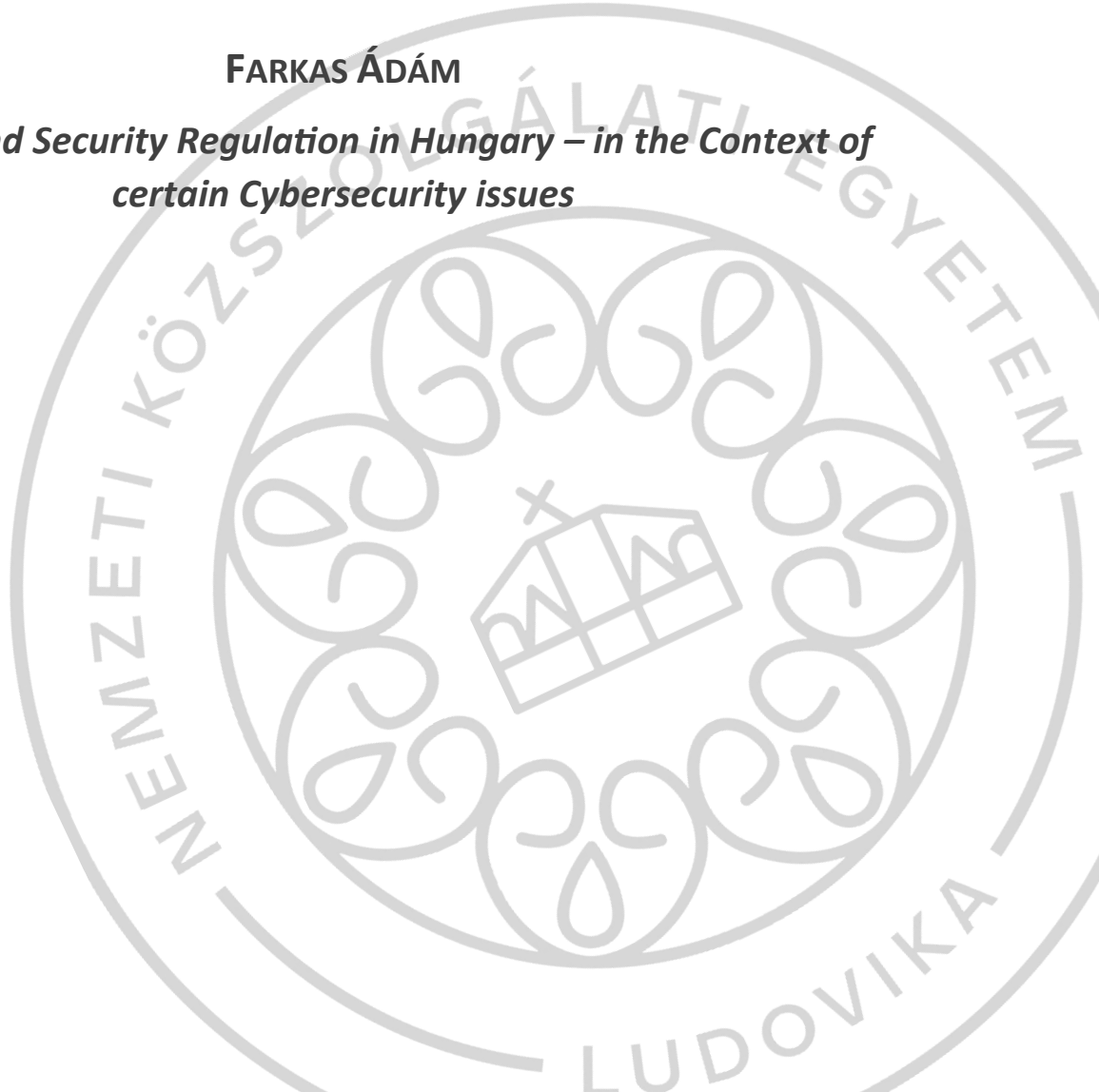
NEMZETI KÖZSZOLGÁLATI EGYETEM
VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY

VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2024/18.

FARKAS ÁDÁM

Defence and Security Regulation in Hungary – in the Context of certain Cybersecurity issues



Rólunk

A műhelytanulmány (working paper) műfaja lehetőséget biztosít arra, hogy a még vállaltan nem teljesen kész munkák szélesebb körben elérhetővé váljanak. Ezzel egyrészt gyorsabban juthatnak el a kutatási részeredmények a szakértői közönséghez, másrészt a közzététel a végleges tanulmány ismertségét is növelheti, végül a megjelenés egyfajta védettséget is jelent, és bizonyítékot, hogy a később publikálandó szövegben szereplő gondolatokat a working paper közzétételekor a szerző már megfogalmazta.

A Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok célja, hogy a Nemzeti Közszolgálati Egyetem Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely küldetéséhez kapcsolódó területek kutatási eredményeit a formális publikációt megelőzően biztosítsa, segítve a láthatóságot, a friss kutatási eredmények gyors közzétételét, megosztását és a tudományos vitát.

A beküldéssel a szerzők vállalják, hogy a mű megírásakor az akadémiai őszinteség szabályai és a tudományosság általánosan elfogadott mércéje szerint jártak el. A sorozatban való megjelenésnek nem feltétele a szakmai lektorálás.

A műfaji jellegből adódóan a leadott szövegekre vonatkozó terjedelmi korlát és egységes megjelenési forma nincs, a szerzőtől várjuk az absztraktot és a megjelentetni kívánt művet oldalszámozással, egységes hivatkozásokkal.

A szerző a beküldéssel hozzájárul, hogy a művét korlátlan ideig a sorozatban elérhetővé tegyük, továbbá vállalja, hogy a working paper alapján megírt végleges szöveg megjelenési helyéről a szerkesztőséget legkésőbb a megjelenéssel egy időben értesíti.

A kiadvány ötletét az MTA Jogtudományi Intézet Law Working Papers sorozatának sikeréből merítettük.

Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2024/18.

Szerző:
Dr. Farkas Ádám

Szerkesztő:
Dr. Kádár Pál dandártábornok

Kiadja
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője
Dr. Kádár Pál dandártábornok

A kézirat lezárva: 2024. október 18.

ISSN 2786-2283

Elérhetőség:
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely
1441 Budapest, Pf.: 60
Cím: 1083 Bp., Ludovika tér 2.
Központi szám: 36 (1) 432-9000

Ádám FARKAS

DEFENCE AND SECURITY REGULATION IN HUNGARY – IN THE CONTEXT OF CERTAIN CYBERSECURITY ISSUES[1]

1. Introduction

The states regulations and their developments in the context of the information era, especially in cyberspace, are in a constant change, due to the novelty of this new phenomena, and the highly differentiated changes in socio-economic-security aspects, as well as the technological background.

In the topic of cybersecurity, it is still an issue that when and how far can states regulate, supervise or intervene. To answer that question, there are quite a few solutions in the international space, however, cybersecurity must be considered alongside cyber operations. These topics ought to be improved and implemented in concert, due to the hard-to-define involvement of civil and public infrastructures and information channels.

This dichotomy is well-seen in the Hungarian regulation as well. In addition to the legal framework for cybersecurity - following EU regulations - there are also legislations for the military cyberspace operations, and for the intelligence services. Cybersecurity in a broad sense, the related powers of public authorities, the regulation of various cyberspace operations, must be intertwined, because of national resilience and the networked nature of cyberspace. To achieve this in the future, the security and safety regulations can provide an appropriate framework in Hungary.

The present study therefore reviews the security and safety legislation adopted in 2021 and in force since 2022 from a broad cybersecurity perspective.

2. Regulation of security and safety activities in Hungary

Since the ninth amendment of the Constitution of Hungary, it has been undergoing a reform of its defense-security regulation. In accordance of this, the first step was to simplify the rules of the special legal order and thus extend the normal tasks of law enforcement. The first step was to simplify the special legal order rules and thus extend the normal legal order protection tasks. This was followed by the adoption of Act XCIII of 2021 on the Coordination of Defense and Security Activities (Act XCIII of 2021) and its entry into force on 1 November 2022. With this, a new, comprehensive regulation has appeared in the Hungarian legal system - similar to the US National Security Act - which is primarily intended to strengthen administrative, law enforcement, military and intelligence cooperation. But the Act XCIII of 2021 could also be the basis for strengthening the coherence needed to enhance cybersecurity.

This is also confirmed by the fact that from the second half of the twentieth century, the concept and notion of security moved away from military dominance towards a complex, sectoral approach. Although the military confrontation and rivalry of the Cold War continued

[1] TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

to give a prominent role to military defense, the intelligence 'war' has also drawn out new center of gravity. Later, the old-new challenges that unfolded at the turn of the millennium, followed by the dynamic development of cyberspace, increased the importance of a broad national security approach. This was confirmed in strategic thinking by the development of the DIME[2] and then MIDFIELD[3] concepts.

The security matrix has thus been extended to a multitude of dimensions and actors of non-military and non-traditional armed characters. This has taken on a new dimension with cyberspace, which means that the state must be prepared to respond to threats in the non-armed spheres in order to protect its citizens and national security interests. This in turn makes the cooperation inevitable between the public and civil sectors, between armed and non-armed forces, and between practitioners and academics. However, it is equally important that the inclusion of non-armed elements in the regulation of defense and security assurance, the development of a coherent planning and training framework and a schema of ideas that can be adopted by decision-makers and the various experts who support their decisions, which will be supported by the ongoing security and defense regulatory reform. Yet this is a considerable challenge, since on the one hand, complexity does not remove the specificities of the field, but builds on them, which inevitably leads to conflicts of vision and interests. In order to achieve thinking and regulating adapted to complex security, first a new kind of mindset is needed, for which, despite the armed character of security-guaranteeing, models can be drawn from the civilian sphere. These patterns can be taken from network research, performance and creativity research, and even from philosophy and political science. This is exemplified by László Barabási-Albert's notion of complexity and its relation to simplification[4], the role of historical and strategic thinking in Christopher Andrew's approach to the history of intelligence[5], Steven Kotler's peak performance research and its view of specialization[6], or David Epstein's work promoting versatility[7]. However, if we are thinking on a deeper level, Arthashastra[8] points towards the inescapability of generalist thinking through its philosophical origins, just as Machiavelli in the Sovereign[9] or Carl Schmitt in his concept of the political, especially with his theory of the partisan[10].

Thus, in interpreting the place and role of the Act XCIII of 2021, it must be acknowledged that security has become a complex concept and thus cannot be dominated by an armed approach and characteristics. Therefore, coordinated defense and security activities also require a complex, generic mindset, which requires the development of specific analytical and proposal-processing capabilities in the coordinating professional bodies, as well as the development of think-tank capabilities separate from the coordinating - practice-based - bodies and their direct involvement in management decision support. These demands are further reinforced by the specific nature of cyberspace, its diverse impacts and the need for specific professional skills.

---

[2] Diplomatic, Informational, Military, and Economic

[3] Military, Informational, Diplomatic, Financial, Intelligence, Economic, Law, and Development

[4] Barabási-Albert László: *Behálózva*. Budapest, Helikon Kiadó, 2008.; Barabási-Albert László: *A hálózatok tudománya.* Budapest, Libri Könyvkiadó, 2016

[5] Christopher Andrew: *Titkos világ I-II.* Budapest, Európa Könyvkiadó, 2021.

[6] Steven Kotler: *A lehetetlen művészete*. Budapest, HVG Könyvek, 2021.

[7] David Epstein: *Sokoldalúság.* Budapest, HVG Könyvek, 2021.

[8] Chanakya Pandit: *Artha-sásztra.* Budapest, Danvantara Kiadó, 2015.

[9] Niccolo Machiavelli: *A fejedelem.* Budapest, Caraphilus Kiadó, 2006.

[10] Carl Schmitt: *A politikai fogalma.* Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.

3. The connections between cyberspace and security and safety regulation

It is also worth comparing the previously mentioned diverse theoretical approach with the approach of the US national security model and the problem of the cyberfare state[11]. From this we can see the horizontal and vertical context in which we need to think when trying to analyse the links of cyberspace to complex state security assurance. This approach, however, requires many years of multidisciplinary research, and readers of this study can only get a glimpse of this in the following context. In order to do that, to create this glimpse, it is also necessary to look at the concrete normative references. In this context, it currently seems self-evident that (1) the identification of Constitutional links and 2) looking at the self-definition of the Act XCIII of 2021, i.e. identifying what role the legislator has placed within the Act - also - reflecting provisions.

With regard to the interconnections and connections of the Act XCIII of 2021 with the Constitution, it is difficult to imagine a detailed and mainly undisputed taxonomy, since the set of norms to which the Act XCIII of 2021 may be connected, at least indirectly, can be imagined as an extremely extensive network, ranging from the contribution to the enforceability of various basic rights, through the connection to the functioning of state bodies, to the special system of legal rules.

At a large number of these points, the connection between cyberspace challenges can be at least implicitly assumed, and at some points necessarily identified, and so the focus of this study is on these connections.

For such an analysis, it may seem appropriate to start from the clause of the Act on the requirements of the Constitution, since it is intended to clearly establish the link with certain paragraphs of the Constitution that impose a priority regulatory requirement.

Article 85 of the Act XCIII of 2021 in the field of compliance with the Constitution

- Article 6. § (1) (a) to (d) and Article 7. § (7) of the Constitution Article XXXI. (4), (5) and (6),
- Article XXXI. (5) of the Constitution in relation to Chapter 4,
- To Chapter 5, Article XXXI. (6) of the Constitution,
- Articles 79-81. §, Articles 52. section (5) and 54. section (8) of the Constitution,
- and to 82. §, Article T (1) of the Constitution,

identifies the linkage, supplemented by the cardinal linkages of the amendments made by the Act XCIII of 2021, in particular in relation to the Hungarian Defense Forces, the police, the national security services and the Parliament.

The legislator himself has thus established a clear link to these provisions of the Constitution, among which the rules of Article XXXI on the obligation to perform military service, the civil defense duty and the obligation to provide economic and material services are particularly important in terms of role definition.

The framework of the Act XCIII of 2021 clearly reflects a comprehensive role that the legislator has set out the provisions that previously appeared simultaneously in the national defense and disaster management legislation in a single framework, as a common rule applicable to these sectors. This change clearly demonstrates the comprehensive nature of the framework for the sectors concerned. To this regulation it is important to add that their

[11] Kelemen Roland: Cyberfare Sate - Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2022/1. szám.

importance in relation to operational activities in cyberspace is not negligible. The nature of the cyber ecosystem and Hungary's connection to the global cyberspace involves a number of non-state actors, for whom this regulation may be relevant in the most serious cases, for example in the event of a large-scale cyberattack.

The involvement of cyberspace in this context is further reinforced by the reference to Articles 52 and 54 of the Constitution, which came into force on 1 November 2022 and were necessary due to the installation of the special legal order in the Act XCIII of 2021. In this context, it is important to highlight that the new specific legal framework has also attempted to be flexible in the grounds for promulgation, taking into consideration the volatility and escalation of the challenges of cyberspace. In this context, the role of cyberspace varies from organized criminal, terrorist, counter-intelligence or military activities to high-impact attacks by non-state actors. The mentioned regulation needs to be responsive to these activities, particularly as their accurate predictability and impact analysis is evolving to this day. In this respect, the role of the Act XCIII of 2021 in the special legal order can be a step forward not only in the complex approach to security, if it is properly enforced and prepared, but also in managing complex cyberspace challenges and threats.

The strong constitutional link in the Act XCIII of 2021 is also demonstrated by the fact that Section 5. § (18) of the Act identifies the Hungarian Defense Forces, law enforcement agencies, national security services and the Parliamentary Guard as defense and security organizations. Point 8 of the same section defines the police, the National Tax and Customs Office, the prison service and the professional disaster management service as law enforcement agencies, so that the Act basically gives their tasks in several points. In relation to this regulation, the close connection between the Act XCIII of 2021 and Articles 45 and 46 of the Constitution is clear. In this manner, the legislator has made the definition of the tasks of the bodies concerned general in the Act XCIII of 2021 and has opened the way for referring solutions in sectoral or organizational regulations. Therefore, the Act XCIII of 2021 also strengthens the cross-sectoral framework for role definition in this area, thereby creating potential ways to more effectively link cybersecurity and cyberspace operational tasks according to sectoral needs.

The involvement of Articles 45 and 46 of the Constitution deserves attention for other reasons as well, since the Act XCIII of 2021, through its regulation focusing on defense and security functions and its overall governmental coordination approach, is directly related to the Government's responsibility for the management of the Defense, Police and National Security Services. On the other hand, however, the ambition to coordinate defense and security activities in a way that is adapted to complex security, and to achieve related coordination and governmental action of a nature that goes far beyond the armed sectors, seems to be clearly linked to Article 15 of the Constitution, and within it to the tasks of the Government. In addition to the coordination character of the complex security, this is also confirmed by Article 46 of the Act XCIII of 2021 with specific provisions for the Government. Following this logic, the link to Article 9 of the Constitution can be clearly identified through the functions of the President of the Republic, and the link to Article 1 of the Constitution both through the provisions relating to the Parliament and indirectly through the special legal order rules. There is a clear cross-sectoral character to the rules and bonds governing, supervising and controlling the coordination of these security and safety activities, compared to the various sectoral laws on security and safety assurance.

In the context of cyberspace security, this cross-sectoral coordination is also of utmost importance, because in addition to the technical aspects of cybersecurity and cyberspace

operations, the coordinated strengthening, development and training of the various human, social and public interfaces is essential for effective cyberspace enforcement. For this purpose, the Act XCIII of 2021 and its institutions can provide a whole-of-government framework if the appropriate application and organizational background is developed.

In addition to the constitutional aspects, which are considered to be significant, we can attempt to identify the main legal elements that may be of particular importance for the definition or interpretation of roles and that can be considered as significant elements in the field of cyberspace security.

In relation to this obligation, the legislator has already given guidance in the preamble, before the specific legislative provisions. When the preamble states that "The National Assembly

- To protect, maintain and develop the security of Hungary and the Hungarian nation, and to promote the interests of Hungary and the Hungarian nation in this context,
- the coordinated and effective management and operation of the capabilities called upon for this purpose,
- to address the multiple and complex challenges and threats of the 21st century security environment,
- coordinated preparedness and defense against threatening, harmful, influencing and offensive behavior based on natural, civilization events and human actions, and
- strengthening a comprehensive approach to crisis management and tasks related to the period of special legal order"[12]

essentially set out its purpose, highlighting the main objectives to be achieved through the proper application of the acquis in this area.

It clearly identifies a framework of goals that aims to promote the maintenance and enhancement of comprehensive security based on passive - i.e. defensive - and active - i.e. advocacy - security through better coordination and harmonization of the various state functions involved. The first two elements are of particular importance in the definition of its role in the Act XCIII of 2021, as the maintenance and development of defense and security is seen in the context of the enforcement of related interests, so that the coordinated and effective management and operation of the relevant capabilities is expected. This is clearly key in the context of cyberspace because of its multiple and diverse uses. It is important to highlight that this approach in the preamble reflects a focus on consistency and governance across the whole spectrum of security. This implies that the legislator is setting out requirements, tasks and operational frameworks in the Act XCIII of 2021, which are built on the regulation of the relevant disciplines. From this point of view, the provisions of the Act XCIII of 2021 can be seen as an element that builds on the sectoral specialties and specific regulation related to cyberspace. This can also promote the appropriate coherence and structuring of cyberspace-related aspects at the political level of governance and in the professional and central decision-making processes that assist it. Examples of such whole-of-government coordination can be found in several NATO member states, from specialized bodies to government offices.

Following the preamble, the legislator stated in Article 1 of the Act XCIII of 2021 that "the defense and security of Hungary is a national matter on which the survival and

[12]Extracts from the preamble of the Act XCIII of 2021

development of the nation, the enforcement of community and individual rights are based, therefore the legal regulations related to the defense and security of the Hungarian nation shall be determined in the light of this Act"[13]. In reference to this provision, it could of course be pointed out that, according to the hierarchy of sources of law, the Act is one law among others, which means that the legislator cannot place it above other relevant legal provisions. The essence of the regulation, however, is rather to define an obligation which the legislator lays down for itself, but which, is imposed on the Government and its specialized bodies as a consequence of the process of preparing legislation by necessity. Therefore, after the adoption and entry into force of the Act, the development of the related legislation should be carried out in the light of the Act. Of course, this does not imply a strict adaptation, since it stipulates that the Act is to be taken into consideration, but it makes it clear that the efficiency and thus broadly defined security objectives set out in the preamble and in the spirit of the links with the Constitution can only be achieved if the related sectoral, organizational and specialized provisions are adapted in future to the new rules at the level of protection and security of the whole government as reflected in the Act. This provision could affect both the future development of existing sectoral regulations in the area of cyberspace protection and security, and the content of a new cybersecurity law to be created in the light of new EU legislation. We believe that if this role of the Act is reflected in newer cybersecurity regulation, it could bring a beneficial change to the current fragmented and weakly cooperative development of cybersecurity and cyberspace operational regulation.

The legislator has clearly confirmed the protection and security system character of the Hungarian legal system, which has been missing until now - not including the rather abstract framework of the protection obligation contained in Article I of the Constitution - by Article 3 of the Act XCIII of 2021. In paragraph (1), on the other hand, it stated that the military defense, law enforcement and national security activities, as separate functional, sectoral and organizational systems, together constitute the system of armed defense of the State. On the contrary, in paragraph 2, it clearly stipulates that the public authorities are obliged to cooperate with them for the purposes set out in Article 1 of the Act. In this way, the Act has clearly and comprehensively linked the key actors of defense and security in the public sphere, both armed and non-armed, in a way that is overarching compared to sectoral/sub-sectoral legislation. This solution is not foreign to the Hungarian legal system, since the broad obligation to cooperate, still related to the system of tasks, appears in the Defense Act, the Police Act and the Act on National Security Services. This solution further strengthens the role interpretation that the Act links the sectors concerned on the one hand, but on the other hand builds on them and at the same time creates new tasks of overall governmental interest above and beyond the sectoral tasks. This aspect may be of particular importance in the context of cyberspace, since on the classical side, actions in cyberspace may trigger a response by armed forces on the basis of strategic declarations by an increasing number of states, while on the practical side, cybersecurity is typically not armed, a duality that can be fully integrated into the approach of the Act. This may open up new perspectives for cooperation coordinated regulation and operational development in the field of cybersecurity and cyberspace operations regulation in Hungary as well.

In our view, the Act's role as a coordinating and interconnecting framework is strengthened by the fact that it sets tasks at the level of the whole government, which is stronger than the coordinating and interconnecting role of the Act. This is reinforced by the

[13] Act XCIII of 2021 1. §

provision in paragraph 20 (2) that "The purpose of the defense and security planning system is to prepare defense and security organizations and bodies under the control of the Government involved in the performance of defense and security tasks for incident management, to strategically define their related operations and development and to provide a framework for cooperation."[14] This interpretation is further reinforced in subsection (3) of the same section, when it states that "the defense and security planning system shall develop strategic and executive-level planning documents, including for the planning of budgetary resources, according to a centralized set of criteria, separately sectoral but coordinated at government level."[15] In this way, the legislator has clearly stipulated that there should be a central set of safety and security requirements for the development of various planning and policy documents. This type of approach could lead to significant progress in the field of cybersecurity, as our country's cybersecurity strategy is already overdue for renewal, both because of the renewal of higher-level strategies and because of the changing environment. In addition, cybersecurity development can be enhanced by strengthening the linkages between cyberspace and national resilience through whole-of-government planning and policy development, also reflected in the Act.

In addition to the above, the specific, whole-of-government nature of the Act, which goes beyond the coordinative framework and provides the basis for policy guidance with a defense and security focus, is best reflected in the tasks of the Government under the Act. In this system of obligations, there are coordinative items relating to the Government's own operation, but beyond these there are also elements that clearly involve obligations and direction. The Government shall perform the tasks set out in Article 46 of the Act in order to ensure the coordinated management of defense and security tasks and, in this context, cooperation with bodies not under its control[16]. In this regard, a more effective national security integration and at the same time a cooperative guarantee of cybersecurity can clearly be facilitated by the following governmental tasks from the list of the Act:

> a) submit to the National Assembly a proposal for a decision on the Basic Principles of Security and Defense Policy and direct the development of further documents for planning for security and defense, [...]
>
> c) determine the tasks of the members of the Government and of the State bodies under the direction of the Government in connection with the preparation and performance of tasks for defense and security purposes; [...]
>
> h) define the programme for the development of national resilience and manage its coordinated implementation,
>
> i) determine the main directions of coordinated preparation and tasking of the Defense Forces, law enforcement agencies and national security services and the framework for exceptional decision-making in this context,
>
> j) defines the tasks of the military and civilian cyberspace operational forces in the context of defense, attack prevention and international operations and

[14] Act XCIII of 2021 20. § (2)
[15] Act XCIII of 2021 20. § (3)
[16] Act XCIII of 2021 46. §

preparations, as well as the framework for exceptional decision-making in this context ..."[17]

By using the terms "directs" and "determines", the legislator clearly intended to build on the Government's function as a governing or top-level state administration, which goes far beyond the scope of coordination. In this context, it is also important to note that each of the tasks highlighted above could be significant in the domestic aspects of more effective state and state-society functioning in cybersecurity. It should also be emphasized that the legislator considered it important to place the issue of the tasks of military and non-military cyberspace operational forces on a separate, uniform basis within the framework of the Act, which serves as a clear umbrella in line with the whole of government approach.

4. Conclusion

The specific legal ties reviewed in the previous sections looked at the ongoing safety and security regulatory reform in Hungary, on the other hand, they wanted to draw attention to its connections and possibilities regarding cybersecurity. It is appropriate to add to all of this that mentioned Act through planning, preparation, national resilience, government-wide defense and security administration, as well as the rules of ordinary state law, order crisis management, the NATO crisis response system, as well as special legal order regulations, it also provides many, many more indirect points of attachment for domestic security activities affecting cyberspace development and more coordinated implementation.

However, all these role interpretations are of a principled nature in that the Act proper functioning over sectors by the Act application, especially its governmental and decision-preparatory application that significantly determines it, will be able to be completed. The Act place and role in the legal system is therefore an groundbreaking promise, also in historical terms, which can be fulfilled by application and then Hungary's defense and security system can enter a new era. In this context, the inclusion of cyber security and cyberspace operational rules and developments in a general government framework will certainly be key.

Therefore, we are currently in the process of developing basic synergies in the field of cyberspace connections of the Hungarian defense and security regulatory reform. The near future holds many opportunities in this regard, since the Act among the new strategies to be developed on the basis of, the cyber security strategy should also be renewed, preferably according to the Act in line with its general government nature. On the other hand, due to the change in EU regulations, it would also be necessary in the new cybersecurity law to strengthen the connections between the specialist field and the Act between the whole government approach. In addition to all this, the dynamic development of cyber security is expected to bring more and more regulatory and operational changes, which are closely related to the overall national security approach, as well as to the sectoral cyberspace operational tasks. The extent to which these will be in sync with the Act by fulfilling the historic promise opened by, the legislation of the following years will show.

[17] Act XCIII of 2021

5. Refrences

[1] Barabási-Albert László: *Behálózva*. Budapest, Helikon Kiadó, 2008.; Barabási-Albert László: *A hálózatok tudománya.* Budapest, Libri Könyvkiadó, 2016.
[2] Carl Schmitt: *A politikai fogalma.* Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.
[3] Chanakya Pandit: *Artha-sásztra.* Budapest, Danvantara Kiadó, 2015.
[4] Christopher Andrew: *Titkos világ I-II.* Budapest, Európa Könyvkiadó, 2021.
[5] David Epstein: *Sokoldalúság.* Budapest, HVG Könyvek, 2021.
[6] Kelemen Roland: Cyberfare Sate - Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2022/1. szám.
[7] Niccolo Machiavelli: *A fejedelem.* Budapest, Caraphilus Kiadó, 2006.
[8] Steven Kotler: *A lehetetlen művészete*. Budapest, HVG Könyvek, 2021.