Ádám Farkas

THE UK'S NATIONAL CYBER FORCE: BEGINNING OF A HYBRID TREND OR NEW ANSWER FOR CYBER DOMAIN

Military and Intelligence CyberSecurity Research Paper
2022/2.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

A tanulmány célja áttekinteni az Egyesült Királyságban 2020 novemberében hivatalosan bejelentett új kiberképesség, a National Cyber Force (NCF) létrehozásából következő egyes kérdéseket. A szerző a napvilágot látott érvek és kritikai észrevételek mellett arra keresi a választ, hogy az NCF egy döntően a kibertér sajátos kihívásaira adott intézményi válasz vagy több annál: egy új trend kezdete a hibrid műveleti környezetben. Ezen kérdésfeltevés mentén a kézirat az NCF kapcsán a hírszerzési és katonai együttműködés, illetve a hírszerző és katonai műveletek metszésében elhelyezkedő tevékenységek kérdéskörét is fókuszba kívánja állítani, mint a hibrid működés sajátos terepét.

Kulcsszavak: kibertér, offenzív képesség, hírszerzés, fegyveres erők, együttműködés

The study aims to review some of the issues arising from the creation of the National Cyber Force (NCF), the new cyber capability formally announced in the UK in November 2020. In addition to the arguments and critiques that have emerged, the author seeks to answer whether the NCF is a decisive institutional response to the specific challenges of cyberspace or more: the beginning of a new trend in the hybrid operational environment. Along the lines of this questioning, the manuscript also seeks to focus on the issue of intelligence-military cooperation and activities at the intersection of intelligence and military operations in the context of the NCF as a specific terrain for hybrid operations.

Keywords: cyberspace, offensive capability, intelligence, armed forces, cooperation

INTRODUCTION

On 19 November 2020, UK Prime Minister Boris Johnson announced a major four-year defence budget increase and capability upgrade, including the *creation of a new Space Command and the National Cyber Force (NCF).*

Subsequently, the NCF received substantial - sometimes critical - attention in several professional platforms. [1] This can be attributed to the combination of intelligence and military tasks in cyberspace, the offensive approach and portfolio, and the mix of tasks ranging from homeland security to military to intelligence, as well as the mix of personnel from these spheres.

[1] Marcus WILLET: *Why the UK's National Cyber Force is an important step forward?*. International Institute for Strategic Studies, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force, letöltve: 2021.03.05.; Danny STEED: *The National Cyber Force: directions and implications for the UK*. Elcano Royal Institute, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk, letöltve: 2021.03.05.; Antonia GOUGH: *UK Government Announces New National Cyber Force*. Global Risk Insight, https://globalriskinsights.com/2021/01/uk-government-announces-new-national-cyber-force/, letöltve: 2021. 03.05.

Nevertheless, in the international context, the *main issues* that can be identified for the NCF are: *(1) the multiagency approach and the fusion of personnel; (2) the outward - offensive - mission; and (3) the organisational and resulting legal specificities.*

Indeed, these issues may go beyond the UK's cyber ambitions and consequent strategic and geopolitical orientation, which in itself is a significant context both in European and global terms.

Moreover, a review of the above questions may lead us closer to answering the question of whether, with this move, the *UK has established a new model and development path or whether it has merely developed a temporary solution* pending clarification of the legal and organisational framework for cyberspace operations across defence and security sectors.

However, it must be examined whether the UK's organisational solution, which can be described as hybrid in both functions and personnel, reflects a pure adaptation to the specificities of cyberspace or whether it goes beyond that to promote a model for more effective action against a wider range of hybrid threats.

The aim of this paper is to review the emergence of the NCF along these lines, as it could provide a possible model or direction of development for several NATO member states, both in terms of institutional and operational cyberspace capability development and regulation, and even in terms of enhancing action against hybrid threats.

Essential Characteristics of the National Cyber Force

A number of key facts about the NCF have been released by the Prime Minister, and then officially by the Government Communications Headquarters (GCHQ) [2], which houses the NCF, following his statement.

This information, and the very fact that a cyberspace operations force with - partly military - functions has been set up on the base of a national security service, in itself suggests an epochal change.

According to UK government communications, the *NCF is a collaboration between GCHQ, as a national security service, and the Ministry of Defence (MoD, including its subordinate armed forces).*

It is staffed by specialists from GCHQ, MoD (and its subordinates), MI6 and the Defence Science and Technology Laboratory, but under a single command. This will ensure that its range of activities will be staffed with military operational expertise (MoD), scientific and technical capability (DSTL), global technical intelligence capacity (GCHQ) and recruitment and agenting (MI6). This in itself therefore makes clear that the underlying rationale is for a cross-functional and cross-organisational collaboration across defence and security functions and organisations, which can adapt to the complexity of cyberspace and the threat matrix it presents.

It is noted that the mission statement has been developed in close coordination

[2] GCHQ: *National Cyber Force transforms country's cyber capabilities to protect the UK.* GCHQ, https://www.gchq.gov.uk/news/national-cyber-force, letöltve: 2021.03.05.

with diplomatic, economic, political and military capabilities, as well as intelligence and law enforcement. In essence, any operation in cyberspace can be considered in this mission statement, from interception to preventing terrorist activities, to detection of high profile child sexual abuse offences, to operational support to military operations in cyberspace, to classical intelligence activities.

In essence, the ***NCF's mission can therefore cover the full range of threats to national security, where their management justifies a cyber operation, whether domestic or foreign.***

It is also noted that the ***NCF is independent of the organisation and functions of the National Cyber Security Centre (NCSC)***, which was set up in 2016 as part of GCHQ, as its remit is clearly focused on the digital defence of the UK. This separation and the terms of reference made it clear that the NCF's purpose is not, or not exclusively, to carry out homeland and defence operations.

This direction of travel was also made clear by highlighting that the UK had previously been a world leader in offensive cyberspace operations at GCHQ - under which term, however, intelligence operations are also included in the context[3] - and was the first to offer such a capability to NATO.

The novelty and hybridity within the defence and security organisational and functional structure is reflected in the fact that the opening of the brief communication on the NCF emphasises that "The National Cyber Force (NCF) is a partnership between defence and intelligence." [4]

The collaborative but in many respects offensive nature of the intelligence, military and homeland security functions and the unified command of the forces of the relevant agencies assigned to work together is therefore an improvement on the UK's previous cyber operational forces. However, it was important to note that, ***as in the past, future cyberspace operations in the UK will be conducted within a legal framework***, which will be provided by the Intelligence Services[5] and Investigatory Powers Act. [6]

OPEN QUESTIONS AND POSSIBLE BACKGROUNDS

The new capability and action made public by this announcement is ***clearly a step forward in terms of defence and security, a change of approach*** and a major geopolitical decision in the digital space[7].

Indeed, the organisation's terms of reference indicate that the ***UK will take an offensive approach to cyber threats*** to its security and national security interests, in addition to the defensive approach it has taken to date, ***but now with a much broader scope than supporting military operations.***

[3] Vö.: GCHQ i.m.

[4] https://www.gov.uk/government/organisations/national-cyber-force/about

[5] Intelligence Sercices Act.

[6] Investigatory Powers Act.

[7] A digitális tér geopolitikai jelentősége kapcsán lásd: Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában*. Budapest, Pallas Athéné Books, 2020.; FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei*. SmartLaw Research Group Working Paper 2021/1.

The portfolio, which covers terrorism, child sexual abuse on the Internet, intelligence, and cyber operational support to military operations, obviously requires expertise in almost all segments of the defence system, but *this goes beyond inter-organisational cooperation through unified command, without calling into question the classical roles of the organisations concerned.*

How these tasks will relate to one another, i.e. which sub-tasks will receive greater attention in proportion within the mission statement, is still an open question and, in many respects, is likely to remain so because of the intelligence component. It seems likely, however, that this internal proportion will be flexible and will be determined by the government in the light of the current security threat and risk assessment. This assumption is further reinforced by the statement of the Director General of MI6 on 30 November 2021, in which he not only broke with the tradition of secrecy surrounding his position, but made clear that in a changing environment the UK intelligence services - and the state more generally - would need to change their approach in a number of ways. The main reasons for this were the inevitability of civil-state cooperation to keep pace with technological developments and the negative changes in the space of great power. However, this paradigm shift, also linked to the United Kingdom, raises serious questions for the rule of law, [8] beyond the correct interpretation of environmental change.

The challenges of cyberspace should in themselves require serious self-reflection on the part of the transatlantic rule of law in order to ensure that the values of centuries of state development are not unduly compromised in the management of the various threats. In my view, it is far from unjustified to reflect on the fact that changes in the technological environment and, with them, the digitalisation of social and state functions may also lead to the question of a new phase in the development of the state. [9] What certainly needs to be considered, however, is to what extent does the model developed by the UK go beyond the challenges of cyberspace and instead represent the start of a trend towards a more effective operational presence in cyberspace, which is a key area for countering hybrid threats?

In the context of hybrid threats, it can be stated that we are dealing today with an old acquaintance, albeit in a new form. [10] In the 20th century, it is clear that the Soviet Union, for example, was a major practitioner of strategic advocacy and instrumentalisation based on non-purely military actions, of ideological-economic influence on other societies. The military application of the maskkirovka and the

[8] PETRUSKA Ferenc – VIKMAN László: *Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából*. In: Military and Intelligence CyberSecurity Research Paper 2021/4.

[9] Lásd: KELEMEN Roland: *Cyberfare State – Egy hibrid állammodell 21. századi születése*. In: Military and Intelligence CyberSecurity Research Paper 2022/1.

[10] Lásd: Williamson MURRAY – Peter R. MANSOOR: *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge, Cambridge University Press, 2012.; Ofer FRIDMAN – Vitaly KABERNIK – James C. PEARCE (ed.): *Hybrid Conflicts and Information Warfare. New Labels, Old Politics.* Boulder-London, Lynne Rienner Publishers, 2019.

subsequent expansion of this approach goes back more than a century. The export of the political revolution in Lenin's thought also reflects a similar narrative. It should be added, of course, that the use of non-military factors to justify or prepare military-strategic objectives or to accompany specific military operations is far from new in world history. Since the time of Sun Tzu, the Taj Kung and Vej Liao-Ce, this approach has been considered classic. The exploitation of state and social specificities in the context of military operations, the use of spies, relations with the population of enemy territories, the influence on supply chains are all subjects that have been present in the literature on warfare and strategic thinking since antiquity. The Indian Arthashastra's approach to the state, intelligence, counter-intelligence and warfare is another example of this, albeit from a more state-organizational perspective. This complex approach, mixing military and non-military elements - and as such hybrid - then increasingly permeated political philosophy and political science, from Machiavelli to Napoleon and Carl Schmitt, which was separate from military thinking. After this historical route we returned to the theory of warfare and opened up a broader horizon than the military dimension of warfare itself, as it appears in Clausewitz's Absolute War and then in Ludendorff's Total War.

Seen in this way, therefore, if hybrid threats are understood as a combined application of military and non-military factors and objectives, it is far from being a new phenomenon at its core. The key issue today is the revolutionary transformation that this phenomenon has undergone, whereby we are now talking about a new generation of warfare and even a radical change in the security environment. *The novelty of hybrid threats "stems from the explosion in the range of non-military factors that have been used in the past, and their emerging strategic dominance, and their growing power as a result of social and technological developments."* [11] *The underlying technological and social development is rooted in digitalisation and its dramatic impact, especially but not exclusively in society. It has fundamentally reshaped the functioning of the state and social and economic processes, from a wide range of interactions at the individual level, through daily habits, to group and societal relations. This has led to an unprecedented rise in the role of non-military factors, which can be used for strategic purposes, including military ones.* Thus, whereas in earlier periods of history these factors had a limited role, as they required a physical presence to be exploited, today, with the physical constraints partially removed by digitalisation, non-military factors play a much greater role than ever before. And if we take this as a major novelty of hybrid threats, the NCF can be seen as a model experiment that goes beyond a response to cyberspace, which in turn opens up a series of serious questions, including the legal implications.

The exact nature of the task implementation is also an open question, especially in the case of outward action. In

[11] FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai,* In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl – Intézményi és jogi kihívások, Budapest, Zrínyi Kiadó, 2019, 132. o.

this respect, *the strict international legal regime for the use of military force abroad - against another state - and the seriousness of the response to military action,* as well as the open questions of the comparability of cyberspace operations to armed attack, make it more obvious to strengthen the operational nature of intelligence. From the aspect of international law, this solution is less critical - or rather less regulated - and, on the other hand, it is also better suited to the vast majority of the tasks identified. Of course an exception to this could be support for specific military operations, where cyberspace operations could share the legal fate of military operations.

The designation of the legal framework also seems to support the logic described above, since it is based on the laws applicable to intelligence services and investigative authorities, which by their very nature suggest that the former will provide a framework for foreign operations and domestic intelligence activities, while the latter will be for domestic and more law enforcement tasks. This dichotomy clearly shows that the normative framework for the use of military force is not identified as a guiding framework at the level of the declarations.

Danny Steed's reflection on these legal aspects suggests that such *a broad set of tasks can be interpreted as a very significant mandate, to which the application of the old legal framework lends an uncertain guarantee.* In essence, the application of the two Acts only provides a basis for ministerial oversight, but cannot provide a detailed regulatory framework because of the novelty of the system of functions. Consequently, the constitutionality and the rule of law would be largely based on the political responsibility of the ministers, which could be called into question by the secret nature of the operations in question.

It can be seen, therefore, that *the growing importance of cyberspace in the context of the NCF and the need to enhance defence and security capabilities and action in this regard is not disputed, but there are questions* - particularly in the legal, ethical and operational dimensions - that remain to be answered.

Of course, this kind of doubt can also be read to some extent in the official communication, which, on the one hand, presented the framework of the new force as a first step, as a start, i.e. it envisaged further development - and even self-provisioning - and, on the other hand, stressed the importance of the legal framework and its synthesis with the effective enforcement of national security interests. The UK government were thus also aware of the uncertainty or contestability of the regulatory environment, but in this respect they appeared to have clearly shifted the new cooperation scheme towards the intelligence model, given the covert/secret nature of the expected operations and the traditional framework for assertion of interests.

Therefore, if the backgrounds are to be considered in the context of the NCF, *it is important that the emphasis on intelligence is given a prominent place. This is presumably due to the fact that intelligence - and counter-intelligence - is at its core a permanent and independent function of peace-warfare, providing operational and information support to diplomacy, government decision-making,*

economic and geopolitical advocacy, and military action, through and beyond its independent functions. This type of tasking is therefore better suited to the constant uncertainty and threat in cyberspace than military action and its legal framework, which is based on peace-war/conflict dualities.

On the other hand, it should also be seen that, although an *increasing number of strategies stipulate that attacks from cyberspace can, at some level, justify a conventional response, in reality a good part of operations are deliberately kept below this level by the parties and thus cannot be properly interpreted within the legal and decision-making framework governing armed confrontation.*

Thirdly, it is also important to take into account that *a significant part of the threats emerging in cyberspace are more suited to new types of threats that are unconventional and linked to non-state actors than to conventional confrontation.* Accordingly, it can be argued that threats in cyberspace, apart from those carried out as direct and overt military operations, are more analogous to the challenges posed by terrorism and transnational organised crime than to the logic of inter-state conflicts. This specificity opens up similar questions, presumably in relation to countering threats in cyberspace, as it does in relation to counter-terrorism. [12]

It should also be stressed that *the new types of security challenges, moving beyond the classical military phase, raise serious questions in terms of both legal, planning and whole-of-government preparedness and response. The hybrid warfare in Ukraine is a clear example,* but - by 2022. However, until 24 February 2022, it did not push direct, state-to-state military confrontation to the fore in diplomatic, international law and political terms, as clear military action opens up the full range of military instruments to be used by the opposing party, which could threaten serious possibilities of escalation. [13] *Thus, the new kind of 'warfare' can also be interpreted as an argument for strengthening the intelligence/national security/investigative character of operational activities in cyberspace.*

Seen from this perspective, therefore, the emphasis on the intelligence/national security character of the NCF does not seem to be a major novelty, since the key role of the national security services in the field of state action

[12] A téma kapcsán lásd: KAJTÁR Gábor: *A nem állami szereplők elleni önvédelem a nemzetközi jogban*. Budapest, ELTE Eötvös Kiadó, 2015.; SPITZER Jenő: *Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.; BARTKÓ Róbert – FARKAS Ádám: *A terrorizmus elleni harc nemzetközi trendjei*. In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020, 115-131. o.

[13] A téma kapcsán lásd: PORKOLÁB Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* In Hadtudomány 2015/3-4., 36-48. o.; RESPERGER István: *A válságkezelés és a hibrid hadviselés*. Budapest, Dialóg Campus Kiadó, 2018.; FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai*. In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020, 132-149. o.

in cyberspace can be identified in many states of the transatlantic area, followed by the development of military capabilities focused on the military segment.

The key innovation is the fusion of expertise across the relevant defence system organisations and its integration under a single command. This kind of progress both recognises the importance of the core tasks of the relevant services, but also highlights that traditional cooperation based on separate chains of command is not sustainable in addressing counter-intelligence efforts in cyberspace due to its time-consuming nature, different legal frameworks and different ministerial subordination. The significant novelty of the NCF, therefore, while reinforcing the primacy of the intelligence character, is perhaps best identified in the fusional nature and acceleration of command decision making associated with cyberspace operations.

SUMMARY

In this context, the establishment of the NCF shows that it represents a significant step forward in the geopolitical thinking on cyberspace and, consequently, on complex defence and security action. It is less obvious, but in my view needs further analysis, whether the NCF can be interpreted as an opening for a new trend in addressing hybrid threats beyond the response to the multiple threats from cyberspace, in terms of the defence and security functions of the state.

It is almost natural that such an innovation, especially given the scale and pervasiveness of digitalisation, should be accompanied by serious questions that remain to be answered and, in the meantime, create uncertainty. However, it is important to see that, on the other hand, openness has a strategic message value, both to UK citizens in terms of protecting them, and to all - potentially adversarial - parties with a stake in the UK in terms of the UK's expected response and actions in cyberspace.

Based on a review of the information available so far and reflections on its possible background, what is new about the NCF is the fusion of expertise and tasks covering almost the whole of the defence system, but under a single command. This opens up serious questions for the future of cyberspace operations. However, it should be stressed that this novelty is clearly developed with a predominance of an intelligence/national security character, which is justified by the relevant international legal framework, the permanent links of intelligence to national interest in the broad sense, and the covert/overt nature of the tasking.

In addition to the observation and evaluation of the developments to be expected in the NCF, it would therefore seem appropriate to further analyse, theorise and reflect on this development for the future, as this move by the UK is likely to have an encouraging effect on other actors both within and outside NATO.

REFERENCES

[1] Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában*. [The geopolitics of digital data. Power and

conflict in the age of big data.] Budapest, Pallas Athéné Books, 2020.

[2] Antonia GOUGH: *UK Government Announces New National Cyber Force.* Global Risk Insight, https://globalriskinsights.com/2021/01/uk-government-announces-new-national-cyber-force/, letöltve: 2021.03.05.

[3] BARTKÓ Róbert – Farkas Ádám: *A terrorizmus elleni harc nemzetközi trendjei*. [International trends in the fight against terrorism.] In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. [A new type of warfare in the second decade of the 21st century and beyond. Institutional and legal challenges.] Budapest, Zrínyi Kiadó, 2020, 115-131. o.

[4] Danny STEED: *The National Cyber Force: directions and implications for the UK*. Elcano Royal Institute, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk, letöltve: 2021.03.05.

[5] FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai*. [Addressing the challenges of so-called "hybrid warfare" and the limits of international law today.] In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. [A new type of warfare in the second decade of the 21st century and beyond. Institutional and legal challenges.] Budapest, Zrínyi Kiadó, 2020, 132-149. o.

[6] FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei*. [Security - Geopolitics - Digitalisation, or the main messages of Amaël Cattaruzza's book "The Geopolitics of Digital Data"] In SmartLaw Research Group Working Paper 2021/1.

[7] FARKAS Ádám: *Komplex biztonság, hibrid konfliktusok, összetett válaszok*. [Complex security, hybrid conflicts, complex responses.] In Honvédségi Szemle 2020/4., 11-23. o.

[8] GCHQ: NATIONAL CYBER FORCE TRANSFORMS COUNTRY'S CYBER CAPABILITIES TO PROTECT THE UK. GCHQ, HTTPS://WWW.GCHQ.GOV.UK/NEWS/NATIONAL-CYBER-FORCE, LETÖLTVE: 2021.03.05.

[9] HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai*. [The emergence phase of hybrid conflicts or the national security aspects of threat detection, prevention and management.] In Honvédségi Szemle 2020/4., 49-64. o.

[10] KAJTÁR Gábor: *A nem állami szereplők elleni önvédelem a nemzetközi jogban*. [Self-defence against non-state actors in international law.] Budapest, ELTE Eötvös Kiadó, 2015.

[11] KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. [The significance of threats from cyberspace in hybrid conflicts and their likely evolution.] In Honvédségi Szemle 2020/4., 65-81. o.

[12] KELEMEN Roland: *Cyberfare State – Egy hibrid állammodell 21. századi születése.* [Cyberfare State - The 21st Century Birth of a Hybrid State Model.] In: Military and Intelligence CyberSecurity Research Paper 2022/1.

[13] KESZELY László: *A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei*. [Possible Governance Models for Comprehensive Action against Hybrid Conflicts.] In Honvédségi Szemle 2020/4., 24-48. o.

[14] Marcus WILLET: *Why the UK's National Cyber Force is an important step forward?.* International Institute for Strategic Studies, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force, letöltve: 2021.03.05.

[15] PETRUSKA Ferenc – VIKMAN László: *Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából*. [A Formidable Intelligence Statement from the Perspective of Legal Vulnerabilities.] In: Military and Intelligence CyberSecurity Research Paper 2021/4.

[16] PORKOLÁB Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* [Hybrid warfare: a new form of warfare or an old familiar one?] In Hadtudomány 2015/3-4., 36-48. o.

[17] RESPERGER István: *A válságkezelés és a hibrid hadviselés*. [Crisis management and hybrid warfare.] Budapest, Dialóg Campus Kiadó, 2018.

[18] SPITZER Jenő: *Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. [Self-defence versus terrorism: the prohibition of violence and the right of self-defence in international law, with special reference to the possibilities of international action against the Islamic State.] Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.

[19] VIKMAN László: *A műveletтervezés jogi feladatai*. [The legal tasks of operation planning.] In Honvédségi Szemle 2021/2, 44-56. o.

[20] Williamson MURRAY – Peter R. MANSOOR: *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge, Cambridge University Press, 2012.

[21] Ofer FRIDMAN – Vitaly KABERNIK – James C. Pearce (ed.): *Hybrid Conflicts and Information Warfare. New Labels, Old Politics.* Boulder-London, Lynne Rienner Publishers, 2019.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/2.

Szerző(k) / Author(s):
Ádám Farkas PhD (dr. jur.)

Kézirat lezárásának ideje / Manuscript closing time:
2022.05.10.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD / Prof. István Resperger PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.