AARMS Vol. 23, No. 3 (2024) 107–124.

10.32565/aarms.2024.3.6

Hacktivists, Proxy Groups, Cyber Volunteers

The Future of Non-State Actors' Involvement in Military Cyber Operations[1]

Csaba KRASZNAY[2]

This paper explores the involvement of hacktivists, cyber volunteers and proxy groups in military cyber operations, with a particular focus on their roles in the ongoing Russian–Ukrainian war. The research aims to analyse the participation of these non-state actors, their legal implications, and how their involvement could influence the strategic, operational and tactical practices of small and medium-sized NATO member states, such as Hungary. Drawing from case studies, literature review and in-depth interviews with Hungarian military intelligence and public administration leaders, the paper formulates two hypotheses: 1. Hacktivist groups, unless integrated into a state's cyber strategy, hinder tactical objectives and raise significant international legal concerns; and 2. Such groups pose a strategic threat to small NATO countries, including Hungary. The findings emphasise the necessity for NATO states to consider how to engage and regulate cyber volunteers effectively, while minimising the risks posed by hacktivist and proxy groups. Additionally, the research underscores the lack of a unified legal framework governing the use of these non-state actors, which complicates their regulation and control in cyberspace conflicts. The paper concludes with recommendations for how NATO states can leverage the openness of civilians to participate in cyber defence while maintaining legal and operational oversight, supporting the involvement of various cyber groups within the framework of international law.

Keywords: *proxy groups, hacktivists, cyber volunteers, cyber warfare*

[1] This paper was supported by the Bolyai János Research Scholarship of the Hungarian Academy of Sciences.
[2] Ludovika University of Public Service, Department of Cybersecurity, e-mail: krasznay.csaba@uni-nke.hu

Introduction

One of the key issues of the Russian–Ukrainian war from the point of view of military science is the use of cyberspace as the fifth operational domain by the warring parties. At the time of the outbreak of the war, a significant number of military experts believed that cyber operations would be crucial to achieving success, given that Russia had been building its capabilities in this direction since the early 2000s and that the operational objectives were to bring Ukraine to its knees as quickly as possible with as little physical destruction as possible. The procedural methods developed in hybrid operations in cyberspace would have served this objective perfectly. However, the successful military defence of Ukraine has set a different direction for this war, and the focus of military research has shifted to the analysis of events in physical space. But this does not mean that cyberspace operations are not present in less spectacular ways in the course of the confrontations and that elements of operations that had not been encountered in practice before are not present.

Since the early 2000s, the literature has addressed the question of how hackers in a war situation can participate in the defence of their country or in offensive operations against other countries, even if they are citizens of a non-belligerent party. This research topic became particularly topical in 2007, when a cyberspace operation was launched against Estonia. The state-of-the-art of the findings on non-belligerent parties, with the contribution of eminent scholars of international law, was the Tallinn Manual 2.0, published in 2017, the relevant points of which will be quoted below. Since the outbreak of the Russian–Ukrainian war in 2022, however, there are a number of events that can be analysed in practice, which are referred to in the Tallinn Manual 2.0 in theory. After the creation of the Ukrainian IT Army, Healey and Grinberg (2022) warned that support for such irregular groups was both contrary to international law and to the practices issued by the UN and accepted by all member states. While this research attitude persists, a number of questions have been raised about the detail. It is worth mentioning, for example, the study of Thøgersen (2023) examining how hackers supporting the Ukrainian IT Army who do not live in Ukraine should be viewed by the countries from which they conduct their operations. She concludes that the relevant points of international law are quite controversial, and that their interpretation requires that as many states as possible express their views on them. A similar conclusion is reached by Chan and Khaw (2024), who examine nation-state behaviour in cyberspace from the perspective of customary international law. The conclusion of their study is that international law needs to become more interdisciplinary, less nation-state-centred and more adaptable to the challenges of the modern age. Smith and Dean (2023) analyse the activities of irregular cyberspace participants, and their findings are very similar. They also raise the research question of whether these groups are automatically considered enemy combatants by virtue of their participation, and how should the use of commercial IT products and services in conflict be classified? Ashdown (2024) analyses how military and civilian cooperation in sharing cyber intelligence can be achieved. In his view, this will happen organically, as it has happened in other operational domains. The conclusion of many articles on the subject

is therefore typically that, until nation states clearly state their views on the involvement of non-belligerent groups, there is a theoretical framework and high-level positions, but no legal consensus on the details.

The high-level objective of this research is to monitor and analyse the cyber operations of Russia and Ukraine, as well as their supporting external parties, and to draw lessons that can be usefully incorporated into the strategic, operational and tactical practices of a small or medium-sized NATO member state. In this particular research, it is examined how belligerents and their supporters in the Russian–Ukrainian war have involved cyber volunteers, hacktivists and other proxy groups in the conduct of military cyber operations and the feasibility of this approach in Hungary as a NATO member state, considering the possibilities offered by national and international law. The paper's aim is not to give a legal analysis, but rather to make proposals from an organisational, cooperative point of view for military and civilian cooperation in the chosen field. For motivation, the last sentences of Ashdown (2024: 323) can be quoted: "However, the value of historical study may be as much in examining the process by which multiple actors collectively (but not always cooperatively) defined those new domains and their roles within them. In doing so, those actors redefined themselves – they 'bent themselves out of shape together'. It is precisely such a process of redefinition that will play out as militaries and private sector actors learn how to collaborate in the production, sharing, and use of cyber intelligence. The choice facing these organizations is whether to pursue coherence and bend, or cling to unity and break."

The first hypothesis is that the involvement of hacktivist groups in offensive military operations hinders rather than helps to achieve tactical objectives, besides raising serious international legal issues, unless they are tasked and directed by military leadership as cyber volunteers. The second hypothesis is that hacktivist groups pose a strategic threat to all small and medium-sized NATO member states like Hungary, even though they have so far been little perceived as such. To support the first hypothesis, case studies are presented, that are available in open sources in addition to a literature review. In selecting the case studies, those cases were chosen that are representative of the activities of the selected groups. The use of open sources is necessary because the "fog of war" is very significant in an active conflict, making it very difficult to find scientifically credible sources. Therefore, the study will rely on sources that are considered trusted in the cybersecurity and military fields, and are considered primary sources. In support of the second hypothesis, in-depth interviews were conducted with Hungarian military, intelligence, public administration and critical infrastructure defence leaders and commanders whose primary responsibility is to lead and coordinate the national cyber defence. In selecting the interviewees, the primary criterion was to interview experts who, by virtue of their position, are primarily responsible for the military and civilian cyber defence of Hungary, as well as for the cyber defence of critical infrastructures that are crucial for the Hungarian economy. In total, 14 interviews were conducted, online, between December 2023 and February 2024. The anonymity of the respondents is important due to their position. This research was supervised by senior researchers from the Institute for Cybersecurity at the Ludovika University of Public Service, and they confirmed that the selected pool of interviewees is

representative. The questionnaire included a number of questions that will be published in other papers, but some of them were specifically designed to gauge respondents' attitudes towards non-state cyberspace actors.

Conceptual and legal background

Clarifying the conceptual background is essential for the implementation of the research. In this paper, those persons and groups are mentioned that are identified as non-state actors in the Tallinn Manual 2.0. According to Rule 33: "International law regulates cyber operations by non-State actors only in limited cases."[3] In this context, the category of Civilians under Rule 91 includes the subjects listed in the study, saying that "civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate".[4] For ease of identification, the groups referred to in the study are classified according to the criteria proposed by Jason Healey in 2012 and refined by Healey and Grinberg (2022). The author has set up the following relationship between state and non-state actors:

1. State-prohibited: The national government will help stop the third-party attack.
2. State-prohibited-but-inadequate: The national government is cooperative but unable to stop the third-party attack.
3. State-ignored: The national government knows about the third-party attacks but is unwilling to take any official action.
4. State-encouraged: Third parties control and conduct the attack, but the national government encourages them as a matter of policy.
5. State-shaped: Third parties control and conduct the attack, but the state provides some support.
6. State-coordinated: The national government coordinates third-party attackers such as by "suggesting" operational details.
7. State-ordered: The national government directs third-party proxies to conduct the attack on its behalf.
8. State-rogue-conducted: Out-of-control elements of cyber forces of the national government conduct the attack.
9. State-executed: The national government conducts the attack using cyber forces under its direct control.
10. State-integrated: The national government attacks using integrated third-party proxies and government cyber forces.

In this study, some key terms are used. First of all, the role of proxy groups is examined. According to Michael N. Schmitt and Liis Vihul, proxy groups in cyberspace are defined as non-state actors acting under the instructions of a state or controlling or directing the actions of a non-state actor, unless the state actor oversteps its authority and influences the

[3] Schmitt 2017: 174.
[4] Schmitt 2017: 413.

non-state actors. Thus, if a state intelligence service influences a hacker, cybercriminal group, loose, informal group, corporation, or even a terrorist, or insurgent group, we can speak of a proxy operation. The point is that while all of this needs to be judged on a case-by-case basis, there should be a clear governance link between the state and the non-state actor.[5] They belong to the State-coordinated and the State-ordered categories.

Moreover, the work hacktivism is also appearing in the paper. There are many sources to explain this term, but it is worth going back to the source, which defines hacktivism as the empowerment of people to make the world aware of injustices and violations of human rights. In other words, to organise the flow of information worldwide, without restrictions or censorship. The word hacktivism comes from Omega and the concept was described by Count Zero. Oxblood Ruffin (2010) added: "Using technology to improve human rights across electronic media." All three were members of the hacker group Cult of the Dead Cow (cDc), and the term itself emerged in the mid-1990s when cDc was also very active in public life.

Hacktivism is made by hacktivists who engage in hacktivism. However, since the 1990s we have seen so many different forms of hacktivism that it is worthwhile to think more broadly about the participants! This is how Tim Jordan and Paul Taylor describe the phenomenon in their book on hacktivism:

> "Hacktivism is the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaching out of cyberspace utilising virtual powers to mould offline life. Social movements and popular protest are integral parts of twenty-first-century societies. Hacktivism is activism gone electronic."[6]

A hacktivist is therefore someone who takes part in a cyberspace action organised around a political ideology that has an impact on the physical world. Hacktivist groups belong to the State-prohibited-but-inadequate and State-ignored categories in this study.

As a subgroup, patriotic hackers are a very important group of hacktivists for military cyber operations. In her book on hacktivism, Athina Karatzogianni describes patriotic hackers as those who fight for the purity of their nation through the clever use of online media. Paradoxically, nationalism as a political ideology appears behind classic hacktivist actions, exploiting the internet as a global media.[7] They belong to the State-encouraged and the State-coordinated categories.

When patriotic hackers officially carry out their activities under state control, they become cyber volunteers. They can be either in the State-executed or the State-integrated categories. Rain Ottis defines this term this way:

---

5 Schmitt–Vihul 2014.
6 Jordan–Taylor 2014: 1.
7 Karatzogianni 2015: 22.

> "People who participate in the cyber militia of their own free will. They do not get paid for their activities, nor do they have a contractual obligation to the militia. They have the right to choose their level of commitment and to leave the militia, if and when they wish. Therefore, volunteer soldiers who join a government-run cyber attack unit are not considered a cyber militia."[8]

The toolbox of hacktivist actions is not nearly as complex as what a state actor with excellent operational planning skills could execute. Moreover, the strength of hacktivist groups lies in their visibility, so they have no interest in keeping the operation hidden, and they typically carry out the act in groups, often not knowing each other, even from very different geographical locations. Conspiracy is therefore not necessarily the goal. Thus, as summarised by Marco Romagna, a hacktivist attack is typically limited to distributed denial of service attacks (DDoS), website defacement and data theft. Occasionally, malicious code may be used, but this has a rather negative resonance in the community.[9]

It is also important to understand the international legislation to the background of this study. Since hacktivists, proxy groups and cyber volunteers have long been present in the academic discourse, there have been numerous studies on how to judge their activities, including in armed conflicts. Perhaps the most important guidance is the clear prohibition of the use of proxy groups in cyberspace operations, as set out in the final report of the United Nations (UN) Group of Governmental Experts (GGE) 2012–2013. The GGE is tasked with reaching a consensus among member states on certain basic cyberspace rules and standards. Paragraph 23 of UN Resolution A/68/98 makes this clear: "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."[10]

The Tallinn Manual, which takes up the international legal interpretation of the use of cyberspace in war, attempts to clarify the rules for the use of proxy groups, hacktivists and cyber volunteers. Rule 17 sets out this requirement most precisely. According to this rule, the activities of non-state actors carrying out cyber operations are attributable to a state when they are acting under the direction of, or under the direction and control of, a state actor and the state actor is aware of and uses the operation for its own purposes.[11]

Rule 69 attempts to define where the boundary of acts that violate international law begins. According to this rule, cyber operations constitute an act of violence if their scale and effect are comparable to non-cyber operations that constitute an act of violence. It is explained that, for example, the mere financing of a hacktivist group does not constitute an act of violence if that group is part of an insurgency against another country.[12] This explains why it can be useful to support in-country hacktivist groups such as Cyberberkut,

---

8 Ottis 2011: 34.
9 Romagna 2019.
10 United Nations General Assembly 2013: 8.
11 Schmitt 2017: 94.
12 Schmitt 2017: 330.

a pro-Russian group within Ukraine that was actively involved in the cyberspace part of the armed conflict in eastern Ukraine before the outbreak of the war in 2022.[13]

Rule 82 further clarifies when a cyberspace operation constitutes an armed conflict and the place of hacktivist groups in it. Armed conflict is defined as hostilities between two states, including actions that involve mere cyber operations. The rule explains that a cyber operation against Estonia in 2007, for example, does not constitute an armed act because there is no evidence that the persons involved were acting under the instructions of a state or that the operation was organised or approved by a state. In addition, it is questionable whether there was any use of weapons at all, i.e. whether the means used constitute cyber weapons. It is therefore clear from the explanation that, although there are many indications of a coordinated operation by intelligence services, the lack of evidence did not allow for an escalation of the response under international law.[14] However, an analysis of the actions carried out during the Russian–Ukrainian war could lead to exact examples of cyber operations that could be interpreted as an armed conflict.

According to Rule 95, in an armed conflict, a person should be considered a civilian until it is clearly established that he or she is not a civilian. In the case of a hacktivist, it is therefore particularly difficult to take any countermeasures as long as he or she is not directly engaged in hostilities.[15] Under Rule 97, however, direct participation deprives him of civilian status. It is explained that if, for example, a hacktivist tries to attack a military command and control system several times in a row, he remains targetable as long as he continues to attack, not only during the specific attack but also between attacks. In fact, if there is a possibility that he or she will continue attacks after a long pause, the hacktivist may remain a target as long as his or her operational capability is maintained. These rules clearly distinguish the activities of cyber volunteers from those of hacktivists.[16]

Cyber volunteers, hacktivists and proxy groups in the Russian–Ukrainian war

Several members of the open-source intelligence community have been actively following the activities of groups emerging from the Russian–Ukrainian war. Perhaps the best-known such collection can be found at Cyberknow. The CyberTracker's update, released on the second anniversary of the war, identified a total of 125 groups, of which 44 groups supported Ukraine and 81 groups supported Russia. Since the beginning of the war, a total of 380 hacktivist groups have appeared on Cyberknow's lists, but a significant number of these have become inactive over the years.[17] In an analysis also published in February 2024, SecAlliance's Riam Kim-McLeod identifies 34 pro-Russian hacktivist groups that have undertaken more than 4,000 attacks in 2023, often with questionable success. This

[13] Koval 2015.
[14] Schmitt 2017: 379.
[15] Schmitt 2017: 424.
[16] Schmitt 2017: 428.
[17] Cyberknow 2024.

information comes mainly from the groups' Telegram channels.[18] By analysing open sources, it is possible to identify groups that are genuinely hacktivist, that act as proxies and that fit into the category of cyber volunteers.

The hacktivists

Hacktivist groups are independent of the control of state organisations, or at least have no conscious connection with any military or intelligence services. This does not mean, of course, that their operations and actions are not influenced by, or at least not known to, law enforcement agencies, but this indirect link does not cross the boundaries of Rule 17 of the Tallinn Manual. Typical examples include groups operating outside Russia or Ukraine, the best known of which is Anonymous. Anonymous is a decentralised group with a common name and visual elements, but each group defines its own operational objectives. Cyberknow's list includes several groups that define themselves as Anonymous, some of which were active long before the war and some of which were created at the outbreak of the war. Anonymous Romania and AnonGhost are older, Anonymous Italia and AltroAnon are newer. None of the analyses link these groups to either the Ukrainian or their own governments, so it is reasonable to assume that they operate along traditional hacktivist lines.

One of the best examples of Anonymous activity is the March 2022 attack on the servers of the Russian media authority Roskomnadzor. As a result, more than 800 gigabytes of data, including 340,000 files, were uploaded to the Distributed Denial of Secrets (DDoSecrets) site. Although details of the operation are not available, the plot is very typical of Anonymous. After hacking into the Internet server of a politically symbolic organisation (the Russian Internet censorship authority), a lot of data is being uploaded in bulk to a non-governmental leak site, which has previously published information that is embarrassing to the U.S. Government.[19] The target does not seem to be relevant from a military point of view, it may be useful from an intelligence point of view, but it is primarily of political use. A review of collection of the tools Anonymous deployed in 2022 shows that they are not necessarily valuable in supporting military operations, and may even be clearly harmful to countries supporting Ukraine.[20] The list includes the following targets:

- hacking printers
- using Conti Ransomware code
- hijacking Russian servers
- hacking the news
- attacking exposed data
- targeting companies who still do business in Russia
- RoboDial, SMS and email spam
- hacks on key Russian holidays and important date hacks

[18] Kim-McLeod 2024.
[19] Brewster 2022.
[20] Fowler 2022.

However, an interesting anomaly in this series is Anonymous Sudan. This group emerged in early 2023 and its activities coincide to a significant extent with the targets of Russian hybrid operations. In addition, the group has publicly aligned itself with several well-known Russian actors, including Killnet. Statements posted on Telegram also openly support Russian activities. Cyberint's analysis has hypothesised, based on several other small indications, that this group is either a covert counterpart of a Russian intelligence service or part of a well-known Russian cybercriminal group.[21] If this hypothesis is correct, the activity of this group goes beyond hacktivism and should be classified as a proxy group.

The proxies

The category of proxies typically includes groups operating within Russia. The link between Russian intelligence services and patriotic hacker groups is not new. Already during the cyberattack against Estonia, the international press and politics almost immediately identified Russia as the state behind the attack, but the Russian Government then and since then has consistently denied its involvement in the operation. Rain Ottis put the available facts like this in 2008:

> "The Russian government has consistently denied any direct involvement in the cyber attacks that hit Estonia in the spring of 2007. To the author's knowledge, this claim is true. It is remarkable, however, that neither is there any proof of measures taken by the Russian government to mitigate the situation. The lack of cooperation in the Estonian investigation indicates that the Russian government is not interested in identifying the attackers and is therefore, in essence, protecting them. In other words, hostile rhetoric from the political elite motivated people to attack Estonia while nothing was done to stop the attacks. This silent consent, however, can be interpreted as implicit state support because, without fear of retribution, the attackers were free to target Estonian systems."[22]

Ottis adds that information about the execution of the attack was shared among the participants in Russian-language forums. The target, the timing, the method of execution and the ideological motivation were precisely defined. In the end, the attack was carried out by the Nashi ("Ours") youth movement led by Konstantin Goloskokov, who denied having received any instructions from Russian officials.[23] Interestingly, in 2016, Ukrainian security agencies referred to Goloskokov as an officer of the Russian military intelligence service, the GRU, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation.[24]

---

21 Cyberint Research Team 2023.
22 Ottis 2008.
23 Lowe 2009.
24 UCMC 2016.

A report by the Russian investigative portal Meduza names Pyotr Levashov as the coordinator of the attack, who "full-time" ran one of the largest unsolicited mail services, Kelihos, until he was arrested in Barcelona in 2017 following an FBI investigation. According to Medusa's sources, Levashov had been cooperating with Russian state agencies since at least 2005 and actively supported some of their operations using Kelihos's infrastructure.[25] In return, he was untouchable, so although the U.S. investigative authorities had already indicted him in 2007, it was impossible to catch him for 10 years.[26]

This operation is very similar to the one performed by the team NoName057(16). An analysis by SecAlliance cited earlier highlights that this team alone was responsible for more than half of the pro-Russian hacktivist attacks in 2023. According to the analysis, its operations are significantly different from those of all other groups, as their operations are continuous, pre-planned, preceded by serious reconnaissance, in an almost military-like order. They engage a wide range of participants through their Telegram channel, whose work is paid for in cryptocurrency, but their source of funding is unknown. Meanwhile, there is not a single person who publicly claims to run the group.[27] The attacks are carried out using a proprietary service DDoSia.[28] One of the group's recognised attacks was launched against the website of the Finnish Parliament when the country announced its accession to NATO. The DDoS attack only caused problems for a short time. This model is very reminiscent of the Nashi story, so although at the time of writing it is not yet possible to prove that it is a proxy group, it is worth watching for new information about the group in the coming years. There is no information on data theft, which is more typical of ransomware groups that are also likely to be collaborating with Russian state agencies. Due to space constraints, the functioning and role of ransomware groups will not be discussed in this paper.

The cyber volunteers

The most obvious cyber volunteer organisation of the groups that have emerged in the war is the Ukrainian IT Army. Unlike other similar organisations, this group was declared to have been created at the call of the Ukrainian Government on 26 February 2022, when the Minister for Digital Transformation, Mykhailo Fedorov called on professionals who wanted to support the Ukrainian cause to join the IT Army, according to Soesanto (2022). The idea itself came from a Ukrainian digital entrepreneur, Yegor Aushev. Telegram, the main communication platform, has hundreds of thousands of subscribers. Based on Smith and Dean's research, a total of 9,547 domain names have been identified as targets in the Telegram channel as of 1 November 2022.[29] The group has been active during the second anniversary of the war, including the successful attack on the Russian Troika system, the fare payment system for public transport in several Russian cities. The successful attack

[25] Turovsky 2018; U.S. Department of Justice 2018.
[26] United States District Court for the District of Alaska 2017.
[27] Antoniuk 2023.
[28] Sekoia TDR et al. 2024.
[29] Smith–Dean 2023.

was announced by the Ministry of Digital Transformation, which clearly indicates that the IT Army is under the control of the Ukrainian Government.[30]

The IT Army is neither part of the Ukrainian army nor the secret service, nevertheless, it is under their control. Its participants support Ukraine's fight but are not under the command of the superiors of the armed organisations, can participate in any operation and can leave the group at any time. No security checks are carried out on members, and the level of operational security during the execution of attacks is nowhere near as high as it would be for a military or intelligence operation. For this reason, operations are designed to be as spectacular as possible, in line with classic hacktivist attacks. While the Estonian Defence League's cyber unit was the forerunner of the IT Army, which is a classic military volunteer reserve unit with the appropriate status and command, the Ukrainian group is an ad hoc organisation that could in time form the nucleus of an Estonian-style solution but is not at that level at present.

Both Soesanto and Smith and Dean point out, however, that the IT Army's operation raises several legal problems. The legal status of cyber volunteers is clear under the Tallinn Manual rules already quoted, as long as they are working in Ukraine. However, it raises several questions if they are carrying out their activities against Russia from the territory of a country that is not a belligerent in this war. In this case, their activities are likely to violate the law of their own country constituting a criminal offence, but there are no reports of active prosecution by the law enforcement agencies of the countries concerned. So unlike the Russian groups, where the state does not assume any apparent association with its own proxy groups, therefore it is very difficult to attribute them, although if it is possible to do so, then a clear violation of international law can be established, the use of cyber volunteers is clarified in international law. They can be considered an insurgent group with all the consequences that entails, except for those who join from other countries, because in their case cybercriminal is the appropriate term, who should be prosecuted ex officio by the authorities of their own country.

Lessons learned for NATO member countries

The experience of the Russian–Ukrainian war has made it necessary for all NATO members to consider what to do with civilians who want to get involved in possible future conflicts. The primary objective is obviously to recruit as many of the best experts as possible into the professional armed forces who can carry out the necessary cyber operations professionally and under appropriate control. The secondary objective is to recruit as many people as possible into the voluntary reserve system who can be available in a trained and controlled manner, in the Estonian model, in the event of a conflict. However, the groups analysed in this study should be handled with care.

Hacktivists, and patriotic hackers within them, are typically difficult to control, their activities often falling under the categories of computer crimes in the national criminal code, following their emotions rather than instructions. It is easy to imagine that their worldview

[30] Fornusek 2024.

is unacceptable to their governments. They cannot be trusted; therefore, it is difficult to share the necessary operational information with them. Typically, they are involved in offensive operations from several countries, which can cause serious international legal and diplomatic problems. It is easy to imagine that their offensive activities could disrupt covert operations conducted by professional intelligence organisations. For this reason, formal contact with hacktivist groups is not recommended. In the meantime, however, it is advisable to exploit the potential of information operations and to influence the activities of these groups in support of the strategic objectives, as long as this does not constitute direct control and does not violate international law.

The use of proxy groups in warfare is clearly prohibited by international law if they carry out acts of violence. In addition, many NATO governments support the Paris Call for Trust and Security in Cyberspace initiative of the French Government, including Principle 8 which explicitly seeks to prevent non-state actors from participating in offensive operations.[31] While there is nothing to prohibit a state from acting as an organising force behind a hacktivist group and thus using it as a proxy, whether in peacetime, hybrid operations, or in war, to the extent that they do not carry out acts of violence, there would be a serious political dilemma and risk in supporting a proxy group alongside existing commitments. For this reason, it is not advisable to pursue this course.

However, based on the Ukrainian experience, supporting cyber volunteers could be an appropriate direction for NATO member states, given that such groups could be a precursor to the voluntary reserve system and then to professional status. In Hungary, discussions have been ongoing since the early 2010s on how to involve civilian professionals in the country's cyber defence. In 2011, the Voluntary Cyber Defence Coalition was founded to bring together interested parties, following the Estonian model. However, in the period since then, it has not been possible to find a legal way for the Hungarian Defence Forces and volunteers to work together. The main obstacle was the creation of a trust-based legal framework, as there was no possibility of establishing a legal relationship with the volunteers that would include the appropriate guarantees for the Hungarian Defence Forces, while the volunteer reserve status was not considered acceptable by the applicants. Since the establishment of the Hungarian Cyber Command within the Hungarian Defence Forces in 2019 and the possibility to recruit professionals even for offensive cyber operations, the involvement of volunteers has become redundant.

However, the experience of the Russian–Ukrainian war shows that a cyber militia outside the organisation and hierarchy of the army, but under the direction and control of the state, may be necessary. For this reason, it is advisable to examine carefully the national regulations relating to the IT Army and to transpose them into the national legal systems of NATO member states. Indeed, surveys in Hungary show that cybersecurity experts are open to participate in military operations. Back in 2010, the openness of young people to become cyber volunteers was assessed. Although the survey is not representative, its respondents were selected from among the attendees of Hungary's most important hacker conference, Hacktivity, so it is indicative of the willingness to cooperate. Of the 187 respondents, 59% said that if their country needed help, they would be available. 55%

[31] Government of France 2018.

of them, meanwhile, had an explicitly negative opinion of the Hungarian Defence Forces.[32] The survey was repeated in 2024 at the University of Pécs, led by Gábor Gyurák, among students who are studying cybersecurity as part of their curricula. Although 14 years have passed between the two surveys, the willingness to support is very similar. 51.6% of the 219 respondents would support Hungarian cyber operations as volunteers. However, the perception of the Hungarian Defence Forces has improved dramatically in the intervening period, with 72.1% of respondents in the new survey having a positive opinion of the military, up from 26% in the previous survey, suggesting that cyber volunteering may, in fact, be the gateway to systemic engagement.[33]

The threat posed by hacktivist groups

So, cooperation with cyber volunteers can be beneficial for military defence, but the question is how big a threat to national security the hacktivist groups pose. The cited SecAlliance research clearly shows that the activity of attack groups in 2023 was primarily directed against countries that are active participants and supporters of the Russian–Ukrainian war. Ukraine is of course in first place with 718 attacks, followed by the Czech Republic with 300, Poland with 298, Sweden with 245 and Germany with 234. At the bottom of the list are Ireland with 2 attacks, Hungary with 5 and Portugal with 6. The low number of attacks may be explained by the lack of interest due to geographical distance, as the two Western countries have small numbers even though Portugal supports Ukraine with tanks and Ireland with trainers, but also by the more sympathetic attitude towards Russia, which is well known in the case of Hungary. This does not mean that the exposure to hacktivist groups in these countries could not change at any time!

Hungary, for example, specifically identifies such groups as a threat to national security in its 2020 National Security Strategy:

> "Technological development and the availability of new technologies are also leading to an increase in the influence of non-state actors that endanger security and are difficult to control within international security policy. They include organised crime syndicates, international terrorist organisations, cybercrime groups, extremist religious communities, private security contractors, certain non-governmental organisations, and other transnational networks. The possible interests and groups behind these organisations may be difficult to identify and could easily serve covert state intentions. This reshapes the security situation of certain regions and makes it confusing and difficult to assess, also representing a challenge for Hungary."[34]

The same is confirmed by a longer series of research launched in 2023 by the cybersecurity research group of the Ludovika University of Public Service, with the aim of providing the scientific basis for the new Hungarian National Cybersecurity Strategy. As part of the

[32] Kovács–Krasznay 2010.
[33] Gyurák 2024.
[34] Government of Hungary 2020.

research series, interviews were conducted with several leaders and commanders who lead cyber defence units in law enforcement and military organisations and are responsible for the cyber defence of critical infrastructures. In total, 8 commanders in national cyber defence and 6 critical infrastructure chief information security officers were interviewed, including some questions on the threat posed by hacktivist groups. The final and detailed results of this research are planned to be published later; however, the original data set is available for further study at the Institute of Cybersecurity of the Ludovika University of Public Service. According to the senior research panel of the Institute, the selection of the subjects represents the focus area in Hungary.

One question of the questionnaire asked respondents to rate Hungary's overall cyberspace exposure on a scale of 1 to 5. The average response was 3.19, i.e. medium exposure, with most respondents explaining that Hungary is currently of little geopolitical interest, with a significant proportion of attacks stemming from its membership of the EU and NATO. The next question asked respondents to name the three most serious threats that Hungary faces from cyberspace. A total of three respondents mentioned the Russian–Ukrainian war as a threat that should be considered from a strategic cyber defence perspective. One respondent directly mentioned the risk of hacktivist groups. Later, they were asked whether they considered hacktivist groups to be a strategic threat to Hungary's cybersecurity. All but one respondent agreed that the new Hungarian cybersecurity strategy should also address the threats posed by such groups. There was also broad agreement that, in general, geopolitical conflicts such as the war between Russia and Ukraine, plus the tension between Israel–Iran or U.S.–China have an impact on the country's cybersecurity.

As the vast majority of respondents have an ex officio right to comment on Hungarian cybersecurity regulations, their unanimous opinion supports my hypothesis that despite the country's apparent less exposure to hacktivist activity, the threat should be taken seriously. The same is true for other NATO member states, e.g. the Irish National Cyber Security Strategy mentions the threat posed by hacktivists to critical infrastructure and public systems, and the Portuguese strategy lists hacktivists among the strategic threats.[35] So, despite the momentary calm, countries' cyber defence organisations need to be ready for situations where large-scale distributed denial of service (DDoS) attacks or data thefts are suddenly launched. As these actions are prepared less covertly, it is not too difficult to obtain information about the attacks, sometimes from open-source intelligence, but this requires conscious monitoring of the hundreds of specific channels.

Conclusions

The two hypotheses of this research were confirmed in the present study. First, hacktivists and proxy groups have become irrevocably involved in armed conflicts. NATO member state adversaries routinely use these groups in their hybrid operations, even in ways that violate international law and are willing to use these groups in wartime as well. NATO

[35] Government of Ireland 2019; Government of Portugal 2019.

member states, including Hungary, see this as a strategic threat, even if they are little affected by the activities of these groups. On the other hand, it was also demonstrated that Western countries and democracies cannot afford to use hacktivists and proxies for several reasons, but learning from the example of Ukraine, it would be a big mistake to waste the openness and ability of thousands of people to participate in the defence of their country. As Sun Tzu wrote in *The Art of War*, "Thus the energy developed by good fighting men is as the momentum of a round stone rolled down a mountain thousands of feet in height. So much on the subject of energy."[36] The organised use of cyber volunteers can show tremendous energy in cyberspace operations without disrupting real covert operations.

Interviews with Hungarian cyber defence leaders have shown that even in Hungary, a NATO member state that is not under attack, hacktivists are taken seriously, and their activities are seen as a strategic threat. In two surveys repeated 14 years apart, we also saw that young non-professional cybersecurity experts are open to participating in cyber volunteering. While neither survey was representative, it is certainly indicative of the responsible leaders in military cyber defence. Further research could be conducted with a similar survey in other countries and a representative survey in Hungary to gauge the views of the roughly 10,000 cybersecurity professionals working in the field. As one of the results of this research, the author and his colleagues will come up with a legislative proposal that would allow the launch of a cyber volunteering scheme in the Hungarian legal environment, within the framework of the forthcoming Hungarian National Cybersecurity Strategy. As Ferenc Kölcsey, the author of Hungary's national anthem, wrote: "Homeland before all else!"

References

Ashdown, Neil (2024): Unity or Coherence: Shaping Future Civil–Military Intelligence Collaboration in the Cyber Domain. In Kwan, Claire – Lindström, Lauri – Giovanelli, Davide – Podiņš, Kārlis – Štrucl, Damjan (eds.): *CyCon 2024: Over the Horizon.* 16th International Conference on Cyber Conflict. Tallinn: NATO CCDCoE, 311–325. Online: https://doi.org/10.23919/CyCon62501.2024.10685631

Antoniuk, Daryna (2023): What's in a NoName? Researchers See a Lone-wolf DDoS Group. *The Record*, 4 September 2023. Online: https://therecord.media/noname-hacking-group-targets-ukraine-and-allies

Brewster, Thomas (2022): An 'Unhappy American' in the Russia–Ukraine Information War Promises a Huge Leak of Data Stolen from the Kremlin's Internet Censor. *Forbes*, 10 March 2022. Online: www.forbes.com/sites/thomasbrewster/2022/03/10/dddosecrets-in-the-russia-ukraine-information-war-promises-a-huge-leak-of-data-stolen-from-the-kremlins-internet-censor/

Chan, Kristy – Khaw, Joseph (2024): Not All Those Who Wander (Over the Horizon) Are Lost: The Applicability of Existing Paradigms of International Law to Cyberspace and the Interpretation of Customary International Law. In Kwan, Claire – Lindström,

[36] Sun Tzu 2006.

Lauri – Giovanelli, Davide – Podiņš, Kārlis – Štrucl, Damjan (eds.): *CyCon 2024: Over the Horizon.* 16th International Conference on Cyber Conflict. Tallinn: NATO CCDCoE, 177–190. Online: https://doi.org/10.23919/CyCon62501.2024.10685595

Cyberint Research Team (2023): *Behind the Mask of Anonymous Sudan: An Analysis.* Online: https://cyberint.com/blog/research/anonymous-sudan-an-analysis/

Cyberknow (2024): *CyberTracker Update 26. Russia–Ukraine War.* Online: https://cyberknow.substack.com/p/cybertracker-update-26-russia-ukraine

Fornusek, Martin (2024): Ministry: Ukrainian Hackers Disrupt Transport Services in Russian Cities. *The Kyiv Independent*, 13 March 2024. Online: https://kyivindependent.com/ministry-ukrainian-hackers-disrupt-payment-system-in-moscow-subway/

Fowler, Jeremiah (2022): *Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks against the Russian Government.* Online: www.websiteplanet.com/blog/anonymous-cyberwarfare-report/

Government of France (2018): *Paris Call for Trust and Security in Cyberspace.* Online: https://pariscall.international/en/principles

Government of Hungary (2020): *Government Resolution 1163/2020 (IV. 21.) on Hungary's National Security Strategy.* Online: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html

Government of Ireland (2019): *National Cyber Security Strategy.* Online: www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

Government of Portugal (2019): *Estratégia Nacional de Segurança do Ciberespaço 2019–2023.* Online: https://files.diariodarepublica.pt/1s/2019/06/10800/0288802895.pdf?lang=EN

Gyurák, Gábor (2024): *A katonai kibertér műveletek lehetséges kapcsolódási pontjai a Pécsi Tudományegyetem kibertérrel kapcsolatos kutatásaihoz.* Nemzetközi Katonai Kibertér Műveleti Konferencia, Szentendre, 7 March 2024.

Healey, Jason – Grinberg, Olivia (2022): *'Patriotic Hacking' Is No Exception.* Online: www.lawfaremedia.org/article/patriotic-hacking-no-exception

Jordan, Tim – Taylor, Paul A. (2004): *Hacktivism and Cyberwars. Rebels with a Cause?* London – New York: Routledge. Online: https://doi.org/10.4324/9780203490037

Karatzogianni, Athina (2015): *Firebrand Waves of Digital Activism 1994–2014. The Rise and Spread of Hacktivism and Cyberconflict.* London: Palgrave Macmillan. Online: https://doi.org/10.1057/9781137317933

Kim-McLeod, Riam (2024): Russia–Ukraine War: Telegram-based Hacktivism in 2023. *SecAlliance*, 27 February 2024. Online: www.secalliance.com/blog/russia-ukraine-war-telegram-based-hacktivism-in-2023

Kovács, László – Krasznay, Csaba (2010): A Digital Mohács. A Cyber Attack Scenario against Hungary. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 3(Special Issue), 49–59.

Koval, Nikolay (2015): Cyber War in Perspective: Russian Aggression against Ukraine. In Geers, Kenneth (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn: NATO CCDCoE, 55–58.

Lowe, Christian (2009): Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters*, 13 March 2009. Online: www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313/

Ottis, Rain (2008): *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: NATO CCDCoE. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Ottis, Rain (2011): *A Systematic Approach to Offensive Volunteer Cyber Militia.* Tallinn: TUT Press.

Romagna, Marco (2019): Hacktivism: Conceptualization, Techniques, and Historical View. In Holt, Thomas J. – Bossler, Adam M. (eds.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Cham: Springer, 1–27. Online: https://doi.org/10.1007/978-3-319-90307-1_34-1

Ruffin, Oxblood (2010): Hacktivism: From Here to There. *Threat Post*, 9 December 2010. Online: https://threatpost.com/hacktivism-here-there-120910/74759/

Sekoia TDR – Amaury G. – Maxime A. (2024): NoName057(16)'s DDoSia Project: 2024 Updates and Behavioural Shifts. *Sekoia*, 1 March 2024. Online: https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

Schmitt, Michael N. ed. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781316822524

Schmitt, Michael N. – Vihul, Liis (2014): Proxy Wars in Cyber Space: The Evolving International Law of Attribution. *Fletcher Security Review*, 1(2), 54–73.

Smith, Margaret W. – Dean, Thomas (2023): The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn: IEEE, 103–119. Online: https://doi.org/10.23919/CyCon58705.2023.10182061

Soesanto, Stefan (2022): The IT Army of Ukraine: Structure, Tasking, and Eco-System. *CSS Cyberdefense Reports*, June 2022. Online: https://doi.org/10.3929/ETHZ-B-000552293

Sun Tzu (2006): *The Art of War.* Minneapolis: Filiquarian Publishing.

Thøgersen, Marie (2023): Obligations of Non-participating States When Hackers on Their Territory Engage in Armed Conflicts. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn: IEEE, 39–54. Online: https://doi.org/10.23919/CyCon58705.2023.10182021

Turovsky, Daniil (2018): "It's Our Time to Serve the Motherland" How Russia's War in Georgia Sparked Moscow's Modern-day Recruitment of Criminal Hackers. *Meduza*, 7 August 2018. Online: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

UCMC (2016): Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations with his Russian Supervisor. *Ukraine Crisis Media Center*, 3 March 2016. Online: https://uacrisis.org/en/40837-sbu-3

United Nations General Assembly (2013): *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98.* New York: United Nations. Online: https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf?token=j2rtp8zdWwLTUkk6bu&fe=true

United States District Court for the District of Alaska (2017): *United States Versus Peter Yuryevich Levashov.* Online: www.justice.gov/opa/press-release/file/956511/dl

U.S. Department of Justice (2018): Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses. *Office of Public Affairs*, 12 September 2018. Online: www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime