SCANDINAVIAN JOURNAL OF MILITARY STUDIES

Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future

RESEARCH ARTICLE

DAN JERKER B. SVANTESSON

SCANDINAVIAN MILITARY STUDIES

ABSTRACT

This article analyzes the contribution to modern warfare that might potentially be made by the "cyber militia" – a body of volunteers undertaking defense-related activities in cyberspace on behalf of a state, with that state's formal recognition, and with some degree of coordination or guidance by that state, but outside the ambit of the state's regular armed forces or national security structure. Through real world examples from cyber warfare and a literary review of the field, this article suggests a definition for such a cyber militia and outlines the roles such a body may play. It also considers how international law may impact the type of cyber militia envisaged above. Account is taken both of relevant law applying outside armed conflict, and the international humanitarian law that applies in situations of armed conflict. The article discusses the possible benefits and challenges following a state's adoption of a formally recognized cyber militia.

CORRESPONDING AUTHOR:

Dan Jerker B. Svantesson

Bond University, AU

dasvante@bond.edu.au

KEYWORDS:

cyber militia; cyber war; cyber conflict; international law; international humanitarian law

TO CITE THIS ARTICLE:

Svantesson, D. J. B. (2023). Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future. *Scandinavian Journal of Military Studies*, 6(1), pp. 86–101. DOI: https://doi.org/10.31374/sjms.195

DOI: 10.31374/sjms.195

INTRODUCTION

When Russia attacked Ukraine on February 24, 2022, the Ukrainians rapidly established a volunteer "IT Army," coordinated to some degree by the Ministry of Digital Transformation. This IT Army has continued to play an active role in the defense of Ukraine.

While the Ukrainian IT Army appears to be a predominantly improvised response to Russia's aggression, this article explores the thesis that states would do well to actively plan and strategize for the potential use of their own initiatives (discussed as "cyber militias" throughout this article) for the future. To achieve this, several legal issues must be addressed. This article identifies and reflects upon four significant and important questions related to the planning and strategizing of cyber militias:

1. How might we usefully define a cyber militia?
2. What are the roles such a militia might perform?
3. What does international law say about the cyber militia?
4. What are the advantages of formally recognizing a cyber militia?

The relevance of these questions stretches well beyond the war in Ukraine, and in evaluating their responses, states are obligated to act within international law. Thus, this article seeks to draw attention both to the significant potential of the cyber militia and to practical and legal issues that arise from their institution – in particular, relevant restrictions imposed on state approaches by international law. It does so by first making a few observations as to how we may define a force of this kind.

There now exists a substantial literature on cyber war and cyber conflict in which some of the questions raised here have already been discussed (see, for example, Schmitt, 2002; Kaska et al., 2013; Ottis, 2010, 2011; Mavropoulou, 2015; Tsagourias, 2016; Liles, 2014; Shackelford, 2011; Brenner & Clarke, 2010; Tinker, 2015; Maurer, 2018). The definition of such a militia itself is one of these questions. In the absence of consensus, there is (as is often the case) more than one sensible manner to set out and categorize such a force; drawing upon some of the definitions and categorizations in the sources noted here, I advance a specific definition below.

Committing to a specific definition of the term "cyber militia" and explaining how such a militia relates to other related actors are necessary steps in facilitating the following discussion. The aim is to shed light on the possible activities of the type of cyber militia discussed here, and to understand the implications of international law regarding the activities of the militia's members. This discussion highlights the diversity of the roles, both offensive and defensive, that a cyber militia, as defined here, can perform. It also brings attention to a number of complex issues arising from the application of certain laws relevant to contexts outside armed conflict and to international humanitarian law applicable in situations of armed conflict. More specifically, remarks are made about the impact of sovereignty, the non-intervention principle, and prohibition of the use of force. Attention is directed at the legal position of a cyber militia under international humanitarian law and the legal issues associated with foreigners serving in such a militia; in respect of the latter, specific mention is made of the obligation of due diligence and a proposed legal reform – a potential Designated Cyber Militia Bill – is advanced. The article then seeks to highlight a selection of advantages of formally recognized cyber militias before ending with some concluding remarks.

From a methodological perspective, the article may be described as a literary review that draws, also, on certain examples of cyber warfare. The sources include a selection of expert comments (see, for example, Väljataga, 2022; Schmitt, 2017; Ginsburg, 2017; Busstra & Theeuwen, 2020; Haataja, 2019), key works by international organizations,[1] a small number of key cases such as the Corfu Channel case of 1949,[2] and some lessons that can be learnt from the experiences of Ukraine – the world's first active war involving a large-scale cyber militia. While the focus is on the current law, some observations regarding ways in which this topic may shape the future directions of the law are also made.

1 See, for example, United Nations (2021a); United Nations (2021b); and United Nations Charter, art 2(1).

2 See International Court of Justice (1949).

DOI: 10.31374/sjms.195

WHAT IS A CYBER MILITIA?

The term "militia" may carry negative connotations for some, perhaps bringing to mind images of an uncontrollable armed mob. However, there is a long tradition of militias playing a significant role in the defensive capabilities of states.

Academic writings on cyber militia, among them the pioneering work by Schmitt (2002), date back more than two decades, and there are several academic journal articles and other works on the topic from the early to mid-2010s (among them Kaska et al., 2013; Ottis, 2011; Ottis, 2010; Mavropoulou, 2015; Tsagourias, 2016; Liles, 2014; Shackelford, 2011; Brenner & Clarke, 2010). There remains, however, no consensus on the definition of the term "cyber militia." Definitions range from Tinker's (2015) succinct "a collection of volunteers organized in some manner to perform operations in or pertaining to cyberspace" to Ottis's (2010) more complex understanding of an ad-hoc or permanent group of volunteers willing and able to use cyber attacks in order to achieve a political goal. Ottis notes:

> The word "volunteers" in the definition refers to 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. (Ottis, 2010)

To this Ottis (2010) adds that the word "political", as used in his definition, "refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc."

While both these definitions are clearly of value, there certainly remain other possible definitions. For the purpose of the discussion in this article, I adopt Ottis's definition as the starting point, adding specific emendations.

First, as discussed in more detail below, I see the role of a cyber militia as considerably broader than merely engaging in "cyber attacks." This also distinguishes my definition from Maurer's interesting discussion of cyber mercenaries, including the cyber militia, as his focus is limited to "offensive cyber operations" (Maurer, 2018, p. 14). The reason I adopt a broader view of the roles of a cyber militia, including both defensive and offensive activities, is to explore the full potential of a cyber militia in modern warfare.

Second, I would add the requirement that the members of the cyber militia undertake defense-related activities in cyberspace on behalf of a state, with that state's formal recognition, and with some degree of coordination or guidance by that state, but from a "grassroots" perspective implying them to be outside the ambit of that state's regular armed forces or national security structure. Maurer (2018, p. 20) usefully distinguishes between three main types of "proxy relationships": *delegation*, *orchestration*, and *sanctioning*. Under that structure, what I discuss as a cyber militia fits within "delegation" – that is, as Maurer has it, a "proxy relationship where the beneficiary [the state] has significant, at least overall or effective, control over the proxy [in our discussion, cyber militia]." As discussed in more detail below in the context of the advantages of formally recognized cyber militias, this limitation is important given the risk that a cyber militia may, intentionally or unintentionally, cause harm provoking escalation in a conflict. The insistence on formal recognition and a degree of coordination or guidance by the beneficiary state plays a role in minimizing such a risk in relation to the type of cyber militia discussed here.

Third, while less important for our discussion, there is nothing in the conventional definition to prevent the members of a militia receiving some financial support or compensation.

Accepting the above, we may define a cyber militia thus: "A cyber militia undertakes defense-related activities (broadly defined) in or pertaining to cyberspace on behalf of a state, with that state's formal recognition, and with some degree of coordination or guidance on behalf of that state but does so outside the ambit of that state's regular armed forces or national security structure. Cyber militias can be ad-hoc, gathering only for a specific occasion, or standing – and there is nothing to prevent the participants from receiving compensation or support, either financial or in the form of training, from the state in question."

DOI: 10.31374/sjms.195

Based on this definition, we can usefully start to compare and contrast a cyber militia to other actors.

First, under the definition adopted here, a cyber militia is different to the type of non-state actor, often criminal in nature, we commonly see reported to be enjoying a symbiotic relationship, and possibly a degree of coordination, with a state while affording that state plausible deniability by the maintenance of some apparent distance to the state in question (Martin, 2022; Maurer 2018, p. 14). Put simply, as defined here, a cyber militia is openly and formally recognized by its patron state and is therefore different to non-state actors of that kind. Second, a distinction can be made between cyber militias and cyber vigilantes, in that the latter are neither acting on behalf of a state, nor with that state's formal recognition or coordination.

Third, under the definition advanced above, a cyber militia is different to the staff of the military and national security branches. Fourth, it is also different to conscripted "cyber warriors" and the type of "cyber home guard' used in, for example, the Estonian Defence League's Cyber Unit (Kaitseliit, 2023) and the Swedish Home Guard ("Hemvärnet") which form part of these countries' national armed forces (Försvarsmakten, 2022). To put this in context, with reference to the U.S. defense structure, the cyber militia discussed in this article is less formalized, specialized, and structured than the National Guard Cyber Defense Team, but more formalized, specialized, and structured than cyber vigilantes and the traditional (ostensible) non-state actors.

THE ROLES OF A CYBER MILITIA

While there have been warnings about the threat of imminent cyberwar (United Nations, 2021a), as the Russian attack on Ukraine intensified in 2022, it was noted that the cyber-dimension of the war was less prominent than many observers had expected (Martin, 2022). The importance of the cyber domain is nevertheless well-established; cyber is also an important facilitator for capabilities in other domains including the maritime, air, land, and space domains. Thus, despite the arguably rather limited cyber-aspect of the war in Ukraine, this should certainly not be mistaken for an indicator that the cyber domain is insignificant.

Given this context, what are the roles one might imagine a cyber militia, as defined above, to be carrying out? To explore that, I have looked at groups sharing certain common characteristics with my definition of cyber militias, among them NAFO ("the North Atlantic Fellas Organization") and the Ukrainian IT Army. I also draw on existing literature on the field, seeking to map out the roles such a structure might play.

As noted by Storm Jensen (2018), a state can principally seek to defend its society in the cyber domain through deterrence, protection and resilience. A cyber militia can play a role in all three through several different types of activities. Here, four such activities are highlighted.

CYBER ATTACKS

As illustrated by the Ukrainian IT Army, a cyber militia may be utilized for the purpose of carrying out cyber attacks, such as distributed denial-of-service (DDoS) attacks, for example, against designated targets (Soesanto, 2022, p. 4). A key feature here, and indeed potentially in relation to most cyber militia activities, is the adoption of a "control by objectives lists" structure: that is, the state in question exercises control over the cyber militia's activities by publishing lists of specific objectives. In such cases, only when acting in the pursuit of those objectives is a person acting as part of the cyber militia as defined above.

In the case of Ukraine, in May of 2022 the Ministry of Digital Transformation claimed that since the Russian 2022 invasion of Ukraine, the Ukrainian IT Army had attacked some 2,000 Russian resources (Soesanto, 2022, p. 7).

Interestingly, it has been reported that cyber criminals that might ordinarily have avoided Russian targets have now directed their efforts at Russia – not for any geopolitical reasons, but, rather, due to the fact that Russian defenses are occupied with war-related cyber attacks and are therefore less able to defend against conventional cybercrime (Menn, 2022). The is not to condone cybercrime; it is to simply highlight the undeniable potential synergies between war-related attacks and conventional cybercrime: each may benefit from the other's impact on the target's capacity to defend itself.

DOI: 10.31374/sjms.195

In the context of the war in Ukraine, the activity of the "Belarusian Cyber Partisans" is also illustrative. It has been reported that this Belarus-based hacktivist group managed to encrypt certain servers, databases, and workstations of the train company Belarusian Railway to interfere with Russian troop movements in Belarus (Väljataga, 2022, p. 1). Without entering any debate about whether the Belarusian Cyber Partisans fit within the definition of a cyber militia, this highlights the diversity of types of cyber attacks in which a cyber militia may engage.

A state being in the position to deploy a cyber militia undertaking targeted cyber attacks may be a significant deterrent.

SYSTEMS SUPPORT

A cyber militia need not be limited to offensive activities such as the cyber attacks discussed above. Where members are properly vetted and trained, they could also be provided with various support roles helping to keep computer systems available and running. For example, on its most basic level, a cyber militia can play a role in helping ensure that citizens in their local area maintain internet access through home networks or the networks of institutions such as local libraries in a time of crisis. Obviously, however, the support of sensitive systems must be kept in the hands of employed experts.

It may here also be noted that a cyber militia engaging in a "systems support role" has utility beyond military conflicts; just as, for example, members of the Swedish Hemvärnet may be called upon to assume a variety of roles to support society in times of crises (natural disasters, for example), members of a cyber militia could be mobilized to provide systems support as the need arises (Försvarsmakten (n.d.). Indeed, here it is appropriate to emphasize that, not least when it comes to the work of a cyber militia engaging in a systems support role, its activities may usefully be coordinated with the work done by a cyber home guard. Indeed, one may imagine structures where the cyber home guard trains and leads the cyber militia in this respect. A cyber militia engaged in the systems support role may contribute both to protection and resilience. Indeed, I would argue that resilience is a form of deterrence, and where that claim is accepted, it may be said that a cyber militia providing systems support contributes towards all three of the ways noted above in which a state can protect society in the cyber domain (Storm Jensen, 2018).

OPEN-SOURCE INTELLIGENCE

A cyber militia can be an important component in open-source intelligence (OSINT) – the collection and analysis of intelligence from publicly available sources. Traditional online OSINT resources include, for example, maps, flight radar trackers, and social media. As the amount of data posted online by both combatants and civilians continues to increase, the role of OSINT is amplified as such content may, for example, reveal enemy positions and troop movements. Beyond traditional OSINT, there is some potential for a cyber militia to engage in the active production of new intelligence through means such as the use of private drones.

Importantly, the OSINT role of a cyber militia may also support evidence-gathering to be used in the future prosecution of war criminals. Even in the early stages of the 2022 Russian invasion of Ukraine, for example, it was reported that Ukraine's Digital Ministry created, and made public, a range of digital tools to crowdsource and corroborate evidence of alleged war crimes (Bergengruen, 2022).

At the time of writing, it is too early to draw any extensive conclusions from the Ukraine war in this respect; much of the evidence collected is yet to be tested in court. But it is already obvious that this type of evidence collection also requires, or at least benefits from, training to ensure that the evidence is collected in a manner that enables the use of the evidence in legal procedures.

A cyber militia operating in the OSINT role may both be a deterrent (hostile activities are more likely to be discovered and recorded, for example) and may facilitate greater protection and resilience.

DOI: 10.31374/sjms.195

INFORMATION WARFARE

It seems clear that states are now in a constant state of information warfare. It has also been noted that, thanks to technological developments, hostile actors have more options available than ever before to influence opinions and processes in foreign states (Commonwealth of Australia, 2021, p. 1).

A cyber militia can counter foreign information warfare by providing both the citizens of the state served by the militia and the outside world a continuous flow of up-to-date, factual, and verified information. While this is significant in times of peace and hybrid warfare, it is even more so in the case of armed conflict when an attacker will seek to cut off "communications between forces in the urban area and their higher command to deny both from knowing the other's status" (U.S. Department of the Army and U.S. Department of the Marine Corps Tactics and Operations Group, 2022, pp. 4–83). A cyber militia may work to counter such isolation.

In more detail, and from the perspective of the defender, it has been noted that urban defense involves "aggressive IO/OIE [information operations/ operations in the information environment] to build civil population support, prevent urban operation interference, and mitigate risk of civilian casualties" (U.S. Department of the Army and U.S. Department of the Marine Corps Tactics and Operations Group, 2022, pp. 5–6). The role a cyber militia can play in this context is obvious: it can provide an important role both in external and internal communications (i.e., communications with higher command and communications within the urban community), not least in an urban warfare scenario.

Remaining in the information field, a final – and perhaps equally important – role for a cyber militia is the influencing of the narrative in both traditional and social media. Again, the Ukraine war is highly illustrative here. Without in any sense downplaying or undermining the importance of the Ukrainian military, it may be argued that the current war may be won or lost in the arena of public opinion of the (mainly Western) states supplying weapons and other forms of support to Ukraine. A cyber militia can be used to steer the narrative, to fact check, and to point out inaccuracies in, and counter, enemy propaganda. Russia, for example, tried to use its announced (but not upheld) unilateral 36-hour ceasefire of 6–7 January 2023 in observance of Orthodox Christmas celebrations as a propaganda tool to tarnish the Ukrainian reputation on the international stage (Institute for the Study of War, 2023). A cyber militia can play a central role in directing the narrative to counter such propaganda, especially in the influential arena of social media. States organizing a cyber militia for such purposes ought to train the members on the propaganda methods of potential adversaries.[3] Relatedly, as highlighted by the debate associated with the highly controversial Amnesty International report published on August 4, 2022 (Amnesty International, 2022), a cyber militia ought to be equipped to monitor the publications of key international bodies and be prepared to present a counter-narrative where it is justified to do so. This requires specialized training.

Discussing information warfare in the Ukraine context, it would be remiss not to mention the so-called North Atlantic Fella Organization.[4] NAFO "is an organic online group of pro-Ukraine supporters that have gained the attention of policymakers and global leaders for their creative use of digital media to take on key sources of Russian disinformation and raise support for the war effort in Ukraine" (Center for Strategic and International Studies, 2022). The work of NAFO is illustrative of some roles that a cyber militia could play even though NAFO, as currently utilized, may not necessarily fit the definition of cyber militia proposed above.

Effective information warfare capabilities, to which a cyber militia clearly may contribute, may arguably serve all three of the ways noted above that a state can protect society in the cyber domain.

THE UNCOMMON CHARACTERISTICS OF SPEED AND LOW COST

To conclude this section, it may be noted that, upon the Russian 2022 attack, Ukraine rapidly developed a range of cyber capabilities – some of which fit within the ways in which this article defines a cyber militia and the roles it is anticipated that such a militia might carry out. While it is

3 For an informed discussion of Russian propaganda, see Wilson (2017).

4 Also known as @Official_NAFO on Twitter.

DOI: 10.31374/sjms.195

impossible to ascertain the exact size, it was reported that the largest number of subscribers of the IT Army's Telegram channel – the key tool for communicating with the IT Army's members – was recorded as 307,165 on March 26, 2022; as of June 10, 2022, the subscriber count was still an impressive 259,225 (Soesanto, 2022, p. 8). While it goes without saying that not every one of these subscribers will actively pursue the IT Army's goals communicated through the Telegram channel, should even a fraction of the subscribers choose to do so, it would constitute a formidable resource nevertheless.

Speed and low cost are indeed uncommon characteristics when it comes to defense measures; the acquisition of military hardware is typically both slow and expensive. In this light, perhaps the most interesting lesson from Ukraine is that, given that it is made up of volunteers, a cyber militia can be created very quickly (in its simplest form, at least), and at a low cost. The same is largely true about a cyber home guard, although, given that it is a formal part of the national armed forces, its establishment may face some additional hurdles.

THE CYBER MILITIA AND ISSUES OF INTERNATIONAL LAW

The fact that law, including international law, applies to the cyber context is now beyond reasonable question. States have, on numerous occasions, reaffirmed consensus around the idea that "international law, in particular the Charter of the United Nations, is applicable, and essential, to maintaining peace, security and stability in the ICT[5] environment" (United Nations, 2021b, A/75/816, Annex I, ¶7). We must begin, therefore, by recognizing that international law applies to a cyber militia, and that, consequently, international law must influence how states structure and use their cyber militias.

As important as this is, it must also be acknowledged that, beyond this very general observation, we soon enter a quagmire of disagreement, uncertainty, and definitional gaps. Put simply, the consensus on the fact that international law applies in the cyber domain is severely undermined by the absence of any consensus as to *how* it might apply.

It is also clear that a cyber militia may operate both inside and outside an environment classed as an armed conflict. Importantly, international humanitarian law applies only in situations of armed conflict (United Nations, 2021a, p. 18). Thus, to understand how international law may impact the type of cyber militia envisaged above, we need to take account both of relevant laws applying outside armed conflict and the international humanitarian law that applies in situations of armed conflict. Notwithstanding that these are, clearly, huge topics deserving of detailed attention, here the ambition is limited to pointing to key issues and providing an initial analysis with the ambition of helping to set the direction for necessary future research.

CYBER MILITIA OUTSIDE THE CONTEXT OF ARMED CONFLICT

The four most obvious aspects of international law that come to mind in the context of a cyber militia, outside the context of armed conflict, concern sovereignty,[6] the non-intervention principle,[7] the prohibition of the use of force,[8] and due diligence. The latter is discussed in some detail below in the context of issues of international law regarding foreigners serving in a cyber militia.

The concept of sovereignty has gained a considerable amount of attention in the cyber defense context (Schmitt, 2017; Svantesson et al., 2021; Svantesson et al., 2023). It is, however, a contested concept, for example, in that there are differing opinions as to whether sovereignty is itself a binding rule or, rather, a principle guiding state interactions without dictating results under international law. Important aspects of the current debate are showcased with great clarity in an excellent Symposium on Sovereignty, Cyberspace, and the Tallinn Manual 2.0 published in 2017 in the American Journal of International Law Unbound (Ginsburg, 2017, pp. 205–206). A third option, in a sense a middle-ground, has also been presented (Svantesson, 2018, pp. 37–39). At any rate, it seems clear that some activities that may be undertaken by a

5 Information and communication technology.

6 *Charter of the United Nations*, 1945, 1 UNTS XVI, Article 2 (1).

7 See United Nations, 1970, p. 123.

8 *Charter of the United Nations*, 1945, 1 UNTS XVI, Article 2 (4).

DOI: 10.31374/sjms.195

cyber militia could infringe upon the sovereignty of another state. Consequently, the potential impact on a foreign state's sovereignty ought to form part of any assessment of the tasks assigned to a cyber militia.

The non-intervention principle is a rule of customary international law and is closely connected with state sovereignty. It prohibits states from using coercive means to intervene in the internal or external affairs of other states. The connection to sovereignty is particularly strong for those who believe sovereignty to be a principle rather than a binding rule. For this school of thought, the principle of non-intervention provides the lowest threshold for cyber operations to constitute violations of international law; cyber activities that do not constitute an intervention, that is, would not be considered to violate international law (Svantesson et al., 2021, pp. 33–36). Most activities in which a cyber militia may engage – the roles of systems support, OSINT, and information warfare, for example – are unlikely to cause any concern under the non-intervention principle. Other types of activities, however, such as cyber attacks aimed at altering election results, may well amount to a prohibited intervention (Egan, 2016). It may be advisable to make sure that the activities assigned to a cyber militia steer well clear of anything that may amount to a prohibited intervention.

The prohibition on the use of force is found in Article 2(4) of the United Nations Charter. While the International Court of Justice has affirmed that it applies "to any use of force, regardless of the weapons employed,"[9] the exact nature of its application in the cyber domain is disputed. However, there seems to be an emerging agreement that "where a cyber operation results in damage or destruction of physical property, or injury or death of human beings, it is likely to be considered to amount to a use of force in violation of article 2(4)" (Svantesson et al., 2021, p. 37; see also Schmitt, 2017, p. 330).

Particular complications arise in a situation where a cyber operation results in loss of functionality without causing physical damage or harm to a system: does this constitute the use of force? (Haataja, 2019, pp. 89–95). Several states, the Netherlands among them, for example, have suggested that a cyber operation with a very serious financial or economic impact may qualify as the use of force (Government of the Kingdom of the Netherlands, 2019, p. 2; Busstra & Theeuwen, 2020, pp. 26–28). This issue requires further attention and must also be debated in the context of the potential operations of a cyber militia.

Beyond the above, there is another way international law and norms as they apply to a cyber militia outside the context of armed conflict, including emergent laws and norms, may possibly be considered. We may usefully assess the potential cyber militia activities against the 11 voluntary, non-binding norms of responsible state behavior in cyberspace developed within the work of the UN's Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, formed to address the security and use of information and communications technologies, and its Group of Governmental Experts on Advancing Responsible state Behavior in Cyberspace in the Context of International Security.

Specifically, it may be noted that some of these norms identify particularly serious conduct. For example, Norm 13 (f) emphasizes that a state "should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (United Nations, 2021a, p. 13). Further, Norm 13 (k) outlines that "states should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams … of another state" (United Nations, 2021a, pp. 16–17). Given their sensitivity, where a state sets out to engage in activities that may relate to, or come into contact with, such matters, a cyber militia should not be used.

CYBER MILITIA IN THE CONTEXT OF ARMED CONFLICT

In the context of armed conflict, the most pressing legal question relating to the type of cyber militia discussed here is that of how militia members are to be categorized under international humanitarian law. While none of the activities anticipated in the text above are likely to place the militia members in the category of combatants, several options remain.

9 International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep 226, p. 244.

DOI: 10.31374/sjms.195

In her excellent discussion of the matter, Väljataga points to two main options: "Depending on the nature of the operations it undertakes and how it is governed and organised, the volunteers in the IT Army can be legally categorised as either civilians indirectly supporting hostilities, [or] civilians directly participating in hostilities" (Väljataga, 2022, p. 2). This categorization seems appropriate also for the type of cyber militia discussed in this article, and I agree with Väljataga's assessment that the third category, that of a *levée en masse* "composed of inhabitants of the territory over which the war is waged but which is not yet occupied by foreign forces"[10] is problematic and is, as she puts it "a stretch too far." Consequently, I focus the discussion on the first two possible categories she mentions.

This categorization carries significance, not least, because civilians that directly participate in hostilities are legitimate military targets under international humanitarian law.[11] As Väljataga notes, this is something to take note of before signing up to join a cyber militia. However, at the same time it may be noted that, given how the Russian attackers have attacked and abused the civilian population in Ukraine, the value of being classed as a civilian is limited in the context of that particular conflict. Furthermore, while Väljataga correctly notes that various operations below the threshold of a cyber attack – including the collection of intelligence on the armed forces (Prosecutor v. Strugar, 2008, ¶177), and the disruption of enemy communications (Bundesgerichtshof, 2010, pp. 59–63) – may bring a person within the category of "civilians directly participating in hostilities," she equally correctly points to several legal obstacles to such a categorization.

First, to fall into the category of "civilians directly participating in hostilities", the activity engaged in must somehow directly contribute to military harm. Otherwise, the perpetrators' civilian immunity remains intact. Most activities of the Ukrainian IT Army seem to have fallen below this threshold. Indeed, states may wish to consider using the standard for civilian immunity as a guiding tool for the type of tasks and objectives they assign to their cyber militias. Second, international law seemingly still favors a presumption against direct participation. Third, as also noted by Väljataga, "retaliatory or preventive use of force against an individual only 'sporadically' participating in hostilities is deemed unlawful" (Väljataga, 2022, p. 3).

In summary, it should be understood that members of a cyber militia – at least as defined in this article – are likely to fall outside the category of combatants. While there is a risk that they may be viewed as civilians directly participating in hostilities in some cases, they would in most cases, on a fair-minded assessment, be considered civilians indirectly supporting hostilities, and thereby avoid constituting legitimate military targets under international humanitarian law.

To conclude this discussion, it may be argued that developments such as the type of IT Army we have seen in Ukraine points to a need for an expansion of the categories noted above. One could, for example, imagine a new specific category of "civilians directly participating in cyber hostilities" in response to which international humanitarian law may allow measures such as "hack back" without such individuals constituting otherwise legitimate military targets. That discussion, however, goes well beyond the scope of this article.

INTERNATIONAL LAW ISSUES WITH FOREIGNERS SERVING IN A CYBER MILITIA

The role of foreign combatants in the war in Ukraine has gained extensive attention (see for example N. K.-T. Habtom, 2022). Here, I focus on the foreign volunteers that joined Ukraine's IT Army rather than on those who joined the physical fighting.

The creation of the Ukrainian IT Army brought attention to the fact that volunteering to join such an organization is an attractive option for many people around the world who want to help Ukraine's fight for humanitarian and/or geopolitical reasons. While exact figures cannot be obtained, it is clear that a significant number of foreigners have taken up the challenge. The legality of doing so may depend on the law of the individual's own state.

When it comes to foreigners serving in a state's cyber militia, both the state enlisting those volunteers and the state from which they originate have legal obligations. The state enlisting foreigners into its cyber militia – like Ukraine has done – may have a responsibility for the

10 See further: Additional Protocol III to the Geneva Conventions, art 4A(6).

11 Article 51(3) of the Additional Protocol I to the Geneva Conventions and Article 13(3) of Additional Protocol II.

DOI: 10.31374/sjms.195

activities of the militia members. A state whose citizens are seen to have been permitted to join a foreign cyber militia may find itself at risk of being directly dragged into the conflict to which those citizens are contributing.

I have outlined a law reform proposal – a proposed Designated Cyber Militia Bill – with the aim of creating an appropriate structure, and legal safeguards, for genuine members of a foreign state's designated cyber militia applicable in a narrowly defined set of circumstances (Svantesson, 2022). A step in that direction is a necessity, I assert, if legal certainty for the individuals and the states involved is to be ensured. Under that proposal (outlined in Appendix 1), a state can declare a foreign cyber militia a Designated Cyber Militia provided that: (a) that state has established the cyber militia; (b) that state has invited foreigners to join its cyber militia; and (c) the foreign state is under armed attack by another state.

Under the proposal, members of such a Designated Cyber Militia are then provided with certain legal safeguards including exemption from civil and criminal liability for otherwise are illegal "hacking" activities such as system interference or accessing a computer system without permission. Under the proposal, however, the militia members only enjoy these safeguards in relation to activities that are: (a) undertaken in their capacity as a member of a Designated Cyber Militia; (b) undertaken based on an order issued by the foreign state in command of the Designated Cyber Militia; (c) defensive in nature.

Under this structure, a government has the power, but no duty, to recognize as legitimate a foreign cyber militia. Thus, a state adopting my proposal has full discretion as to when it activates the anticipated legal safeguards for its citizens joining the foreign cyber militia. Under this approach, the starting point is that individuals are prevented from joining a foreign cyber militia to the extent that their activities fall foul of cybercrime laws (or other laws) and can only enjoy the relevant legal safeguards where their government has recognized the activities of the foreign cyber militia as being valuable.

A key challenge in this context comes from the obligation of due diligence articulated by the International Court of Justice's Corfu Channel judgment, according to which "it is every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states" (International Court of Justice 1949, p. 22). Clearly, as already discussed, a cyber militia could undertake hostile acts contrary to the rights of other states. Where a state has knowingly allowed its territory to be used for acts that may be contrary to the rights of other states, it may violate the due diligence principle.

To address this potential concern, I have limited my proposal to covering only activities that are defensive in nature, since these can be limited to activities that do not contravene the rights of other states. However, for clarity, states may define for themselves what they accept as "defensive" activities.

Finally, a few observations may be in order as to the potential consequences of violating due diligence. As observed by Väljataga:

> Having established that another state has failed to exercise due diligence in preventing the harm and investigating the cyber attacks being carried out in its territory, the target state can respond to a breach of sovereignty or prohibited intervention by, for example, imposing sanctions, damaging or disrupting the systems from where the attacks are launched, blocking internet traffic from certain countries, expelling diplomats or some other unfriendly or unlawful action not amounting to the use of force. Stemming from the principle of necessity, any response can only serve the objective of stopping the ongoing cyber operation and not that of deterrence, punishment or prevention. (Väljataga, 2022, p. 5)

In a situation such as that in Ukraine, states may well see these consequences as a price they are willing to pay to support the defending state.

CYBER MILITIA STRUCTURES

A further matter to consider relates to whether there are ways to formalize, and harmonize, cyber militia structures with likeminded states in a mutually beneficial manner, including in situations where the citizens of one state serve in the cyber militia of another. The core of that

DOI: 10.31374/sjms.195

issue is not strictly speaking a legal concern but, rather, practical, and organizational in nature; there are clear synergies that could be exploited for mutual benefit especially amongst states that already cooperate in a defense setting.

Nevertheless, in the context of international law, it may be noted that there are frequent calls for cooperation, and that the type of cooperation hinted at above may – not least where it decreases state reliance on vigilantes and non-state actors – be viewed as a measure "to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security" (United Nations, 2021a, p. 8).

ADVANTAGES OF A FORMALLY RECOGNIZED CYBER MILITIA

It is undeniably already the case that some citizens of various states voluntarily engage in the types of activities that may be undertaken by a cyber militia. However, there are at least three strong reasons why states ought to implement legal structures facilitating a formally recognized cyber militia.

First, doing so will enhance efficiency. An organized, well trained, and properly led, cyber militia will amount to a more powerful tool than uncoordinated actions by volunteers acting on their own initiatives. This is a strong incentive for the creation of a formally recognized cyber militia.

Second, a formally recognized cyber militia ensures a higher level of transparency and accountability than what we are currently seeing in relation the cyber activities of non-state actors, including vigilantes and cyber criminals, that are more or less coordinated by states. The need for transparency and accountability has been emphasized several times, including in a 2021 report by the United Nations' Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (United Nations, 2021a), which noted: "States must not use proxies to commit internationally wrongful acts using ICTs (information and communications technology), and should seek to ensure that their territory is not used by non-State actors to commit such acts."

Third, where a state is willing to adopt, and benefit from, the work of a cyber militia, it ought to provide appropriate legal safeguards for the participants of that militia. Thus, a practice of states designating individuals as members of their cyber militia has direct benefits for the individuals in question.

These three may be viewed as the core reasons why states ought to implement legal structures facilitating a formally recognized cyber militia. However, numerous other, and indirect, benefits may also be foreseen. For example, the capacity of a state to produce a cyber militia depends to a great extent on the ICT-literacy of its population. Consequently, the aim of creating a strong cyber militia may be an incentive for a general increase in ICT-literacy, potentially counteracting some of the existing "digital divides" plaguing many, if not most, societies.

While the risk that a cyber militia may intentionally or unintentionally cause harm that leads to escalation in a conflict cannot be eliminated, it can, however, be minimized where the militia members undertake defense-related activities in cyberspace on behalf of a state, with that state's formal recognition, and with some degree of coordination or guidance by that state. This brings us back to the definition of the cyber militia: a workable definition of the kind set out in this article can directly mitigate this risk.

So far, the discussion in this section has mainly centered on the advantages to be gained by states and individuals implementing legal structures facilitating a formally recognized cyber militia. I would argue, however, that there is one – arguably much greater, but admittedly more controversial – reason why we ought to encourage states to adopt a formally recognized cyber militia: such a force may be a defensive tool useful in leveling out the "attacker advantage" currently enjoyed by aggressors in cyberspace. It is well understood that the internet ecosystem was (predominantly) not constructed with security in mind, and complications associated with attribution further contribute to making the cyber domain an environment advantageous to the attacker (United Nations, 2021a; Maddocks, 2019; Nye, 2016, pp. 49–52; Maurer, 2018, pp. 22–25). Regrettably, despite current cyber capabilities, most, if not all, states are still far from ensuring their cyber defenses are on an equal footing with cyber attackers. Until we reach at least an equilibrium between offensive and defensive cyber capabilities, increased retaliatory

DOI: 10.31374/sjms.195

capacities – while they come with their own set of problems, including the risk of escalation – represent a plausible alternative. Put simply, adding the deterrence of a well-trained, well-organized, and well-directed cyber militia to existing cyber capabilities may alter a potential attacker's cost-benefit calculation and raise a barrier sufficient to prevent the attack in the first place. In this sense, the deterrence capability of a cyber militia may be seen as one aspect in the bigger picture of small and medium size states seeking cost-effective ways to ensure deterrence (Hammes, 2019).

CONCLUDING REMARKS

The 2022 Annual Progress Report from the United Nations' Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies notes that "the use of ICTs in future conflicts between states is becoming more likely" (United Nations, 2022, A/AC.292/2022/CRP.1). I am prepared to go one step further and say that the use of information and communication technology in future conflicts between states is *inevitable*.

To date, both our technological development and our technological dependence have by far outpaced our technological resilience. As correctly noted by Storm Jensen (2018), "'resilience' in this regard describes societal robustness – not only to deflect outside pressure, but also to absorb its effects and constantly adapt to changing conditions by collecting knowledge of negative events, learning from it and implementing the experience."

With continuing ICT uptake across society, there is a corresponding expansion of the "attack surface" vulnerable to malicious cyber activities. A cyber militia can play a role in both the defense, and exploitation, of that expanded attack surface. But in doing so, compliance with international law is paramount for the legitimacy of such activities, and the regulation of cyber militias ought to be an important component of the evolving framework for responsible state behavior in the use of ICTs.

Discussing these issues is urgent, not least given how the brutal Russian invasion of Ukraine has shaken international law in many ways. Daily reports of war crimes and an impotent response by the United Nations suggests that there will be many lessons to be learnt from this war. The efficient prosecution of war criminals will be essential for the future credibility of international law and current international institutions.

In this article, I have suggested a quite specific definition of cyber militias, both to prompt a discussion of international law regulations and to underline the kinds of potential offered by such a structure to modern warfare, in which cyber plays an increasingly important role. I have argued that cyber militias, understood in the way this article proposes, can be a valuable asset to states, both in support of the regular and home guard cyber defense, and for utilization in some types of activities that go beyond the scope of these more traditional and "heavy" institutions. In this, the article does not attempt to be exhaustive; rather, it draws attention to four specific activities in which a cyber militia may engage in support of the goals of deterrence, protection, and resilience. Those activities are cyber attacks, systems support, open-source intelligence, and information warfare.

The article has also sought to bring attention to the key international law issues, both those concerning relevant laws applying outside armed conflict and those concerning the international humanitarian law that applies in situations of armed conflict. Specifically, focus was placed on the impact of sovereignty, the non-intervention principle, the prohibition on the use of force, and the legal position of a cyber militia under international humanitarian law. In addition, the legal issues associated with foreigners serving in a cyber militia were examined taking account of the obligation of due diligence, and a law reform proposal – a potential Designated Cyber Militia Bill (presented in full in Appendix 1) – was advanced.

Finally, the article sought to highlight a selection of advantages of formally recognized cyber militias, including enhanced efficiency, a higher level of transparency and accountability, benefits for those who join a cyber militia, and the fact that a cyber militia may be a defensive tool that can help to level out the advantage an antagonist currently enjoys in attacks made in cyberspace.

DOI: 10.31374/sjms.195

Obviously, a publication in this format can only begin to highlight the issues that require further attention, and it is clear that much work lies ahead. This article's proposition, one among many possible perspectives, is that a thoughtful regulation of the cyber militia can create a degree of accountability, certainty, and oversight that not only strengthens important defensive capabilities, but also works to safeguard peace by raising the cost associated with aggressions in cyberspace, ultimately deterring cyber aggression.

APPENDIX 1 – PROPOSAL FOR A "DESIGNATED CYBER MILITIA BILL"

ARTICLE 1

The government of the state adopting this law can proclaim a foreign cyber militia a Designated Cyber Militia under the following circumstances:

1. The cyber militia has been established by a foreign state;
2. That foreign state has invited foreigners to join this cyber militia; and
3. The foreign state is under armed attack by another state.

ARTICLE 2

Unless the activities constitute a violation of international law, a recognized member of a Designated Cyber Militia enjoys the protection of the legal safeguards outlined in Articles 3–5 in relation to activities that are:

1. Undertaken in their capacity as a member of a Designated Cyber Militia;
2. Undertaken based on an order issued by the foreign state in command of the Designated Cyber Militia; and
3. Defensive in nature.

ARTICLE 3

A person classed as a genuine member of a Designated Cyber Militia under Article 2 is exempt from criminal liability under the following provisions:

[Relevant legal provisions from domestic law]

ARTICLE 4

[The state adopting this law] will refuse any extradition request received where it relates to the activities of a person classed as a recognized member of a Designated Cyber Militia under Article 2.

This does not prevent [the state adopting this law] cooperating in the case of allegations of war crimes being brought against the person before a recognized international war crimes tribunal.

ARTICLE 5

A person classed as a recognized member of a Designated Cyber Militia under Article 2 is exempt from civil liability in relation to activities carried out in that capacity.

FUNDING INFORMATION

The research was supported by Masaryk University project no. CZ.02.1.01/0.0/0.0/16_019/0000822 (C4E). Any views or opinions expressed in this article are personal and do not represent those of institutions or organizations that the authors are associated with in their professional capacity.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATIONS

Dan Jerker B. Svantesson orcid.org/0000-0003-2106-5594
Professor, Faculty of Law, Bond University, AU; Research fellow, Masaryk University, CZ;
Associated Researcher, Swedish Law & Informatics Research Institute, Stockholm University, SE

REFERENCES

Additional Protocol I to the Geneva Conventions of 12 August 1949. (1977, June 8). Retrieved from https://www.icrc.org/en/doc/resources/documents/misc/additional-protocols-1977.htm

Additional Protocol II to the Geneva Conventions of 12 August 1949. (1977, June 8). Retrieved from https://www.icrc.org/en/doc/resources/documents/misc/additional-protocols-1977.htm

Additional Protocol III to the Geneva Conventions of 12 August 1949. (2005, June 8). Retrieved from https://ihl-databases.icrc.org/en/ihl-treaties/apiii-2005

Amnesty International. (2022, August 4). *Ukraine: Ukrainian fighting tactics endanger civilians*. Retrieved from https://www.amnesty.org/en/latest/news/2022/08/ukraine-ukrainian-fighting-tactics-endanger-civilians/

Bergengruen, V. (2022, April 18). How Ukraine is crowdsourcing digital evidence of war crimes. *Time*. Retrieved from https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

Brenner, S. W., & **Clarke, L. L.** (2010). Civilians in cyberwarfare: Conscripts. *Vanderbilt Journal of Transnational Law*, *43*(4), 1011–1076.

Bundesgerichtshof [Federal Court of Justice]. (2010, April 16). Case No. 3 BJs 6/10-4.

Busstra, M., & **Theeuwen, W.** (2020). International law in the context of cyber operations. In *Collected papers van de Koninklijke Nederlandse Vereniging voor Internationaal Recht – nr 147 · International Law for a Digitalised World*. Asser Press.

Center for Strategic and International Studies. (2022, October 5). NAFO and winning the information war: Lessons learned from Ukraine. Retrieved from https://www.csis.org/analysis/nafo-and-winning-information-war-lessons-learned-ukraine

Commonwealth of Australia. (2021, December). Select committee on foreign interference through social media – First interim report. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024741/toc_pdf/FirstInterimReport.pdf;fileType=application%2Fpdf

Egan, B. (2016, November 10). Remarks on international law and stability in cyberspace. US Department of State. Retrieved from https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

Försvarsmakten. (2022, October 4). Frivilligrörelsen får uppdrag inom cyberförsvar och cybersäkerhet. Retrieved from https://www.forsvarsmakten.se/sv/aktuellt/2022/10/frivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhetfrivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhet/

Försvarsmakten. (n.d.). Swedish Home Guard ("Hemvärnet"). Retrieved from https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/hemvarnet/

Ginsburg, T. (2017). Introduction to symposium on sovereignty, cyberspace, and Tallinn manual 2.0. *AJIL Unbound, 111*, 205–206. DOI: https://doi.org/10.1017/aju.2017.58

Government of the Kingdom of the Netherlands. (2019, July). Document sent by Minister of Foreign Affairs to Parliament. Retrieved from https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf

Haataja, S. (2019). *Cyber attacks and international law on the use of force: The turn to information ethics*. Routledge. DOI: https://doi.org/10.4324/9781351057028

Habtom, N. K.-T. (2022). The composition and challenges of foreign fighters in Ukraine. *Scandinavian Journal of Military Studies, 5*(1), 79–90. DOI: https://doi.org/10.31374/sjms.151

Hammes, T. X. (2019). Defending Europe: How converging technology strengthens small powers. *Scandinavian Journal of Military Studies, 2*(1), 20–29. DOI: https://doi.org/10.31374/sjms.24

Institute for the Study of War. (2023, January 5). Russian offensive campaign assessment. Retrieved from https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-5-2023

International Court of Justice. (1949, April 9). Corfu Channel case (I.C.J. Reports, 4).

International Court of Justice. (1996). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep 226.

Kaitseliit. (2023). Estonian Defence League's Cyber Unit. Retrieved from https://www.kaitseliit.ee/en/cyber-unit

Kaska, K., Osula, A.-M., & **Jan Stinissen, L. T. C.** (2013). The cyber defence unit of the Estonian Defence League – Legal, policy and organisational Analysis. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

Liles, L. (2014). The civilian cyber battlefield: non-state cyber operators' status under the law of armed conflict. *North Carolina Journal of International Law and Commercial Regulation, 39*(4), 1091–1122.

Maddocks, J. (2019). Outsourcing of governmental functions in contemporary conflict: rethinking the issue of attribution. *Virginia Journal of International Law, 59*(1), 47–96.

Martin, C. (2022, March 2). Ukraine crisis – Cyber realism in a time of war. Lawfare Blog. Retrieved from https://www.lawfareblog.com/cyber-realism-time-war; https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

Maurer, T. (2018). *Cyber Mercenaries*. Cambridge University Press. DOI: https://doi.org/10.1017/9781316422724

Mavropoulou, E. (2015). Targeting in the cyber domain: Legal challenges arising from the application of the principle of distinction to cyber attacks. *Journal of Law & Cyber Warfare, 4*(2), 23–93.

Menn, J. (2022, May 1). Hacking Russia was off-limits. The Ukraine war made it a free-for-all. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/

Nye, J. S., Jr. (2016). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. DOI: https://doi.org/10.1162/ISEC_a_00266

Ottis, R. (2010, July). Proactive defence tactics against on-line cyber militia. In *Proceedings of the 9th European Conference on Information Warfare and Security*, *Thessaloniki, Greece*. Reading Academic Publishing Limited, pp. 233–237. Retrieved from https://ccdcoe.org/library/publications/proactive-defence-tactics-against-on-line-cyber-militia/

Ottis, R. (2011). Theoretical Offensive Cyber Militia Models. In *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington, DC. Reading Academic Publishing Limited, pp. 307–313. https://ccdcoe.org/library/publications/theoretical-offensive-cyber-militia-models/

Prosecutor v. Strugar, Case No. IT01-42-A, Appeal Judgement, ¶ 177, 17 July 2008.

Schmitt, M. (2002). Wired warfare: Computer network attack and international law. *International Review of the Red Cross, 84*(846), 365–399. DOI: https://doi.org/10.1017/S1560775500097741

Schmitt, M. (Ed.) (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. DOI: https://doi.org/10.1017/9781316822524

Shackelford, S. J., & **Andres, R. B.** (2011). State responsibility for cyber attacks: competing standards for growing problem. *Georgetown Journal of International Law, 42*(4), 971–1016.

Soesanto, S. (2022). The IT Army of Ukraine: Structure, tasking, and ecosystem. Centre for Security Studies. Retrieved from https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/i/the_it_army_of_ukraine

Storm Jensen, M. (2018). Sector responsibility or sector task? New cyber strategy occasion for rethinking the Danish sector responsibility principle. *Scandinavian Journal of Military Studies, 1*(1), 1–18. DOI: https://doi.org/10.31374/sjms.3

Svantesson, D. J. (2018). "Lagom Jurisdiction": What Viking drinking etiquette can teach us about internet jurisdiction and Google France. *Masaryk University Journal of Law and Technology, 12*(1), 29. DOI: https://doi.org/10.5817/MUJLT2018-1-2

Svantesson, D. J. (2022, March 23). Legal safeguards for the volunteers of Ukraine's cyber militia. Verfassungsblog on Matters Constitutional. Retrieved from https://verfassungsblog.de/legal-safeguards-for-the-volunteers-of-ukraines-cyber-militia/

Svantesson, D. J., Azzopardi, R., Bonython, W.E., Crowe, J., Freeland, S. R., Haataja, S., Ireland-Piper, D., & **Mark, N.** (2021). The developing concept of sovereignty: Considerations for defence operations in cyberspace and outer space. Technology and Jurisdiction Research Team Law Faculty Bond University. Retrieved from https://bond.edu.au/files/5701/TheDevelopingConceptofSovereignty.pdf

Svantesson, D. J., Haataja, S., Ireland-Piper, D., & **Chen, K.-W.** (2023). On sovereignty. *Masaryk University Journal of Law and Technology, 17*(1), 33–85.

Tinker, P. (2015). Dor the common defense of cyberspace: Implications of a US cyber militia on Department of Defense cyber operations [Master's thesis]. U.S. Army Command and General Staff College. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA623946.pdf

Tsagourias, N. (2016). Non-state actors, ungoverned spaces and international responsibility for cyber acts. *Journal of Conflict and Security Law, 21*(3), 455–474. DOI: https://doi.org/10.1093/jcsl/krw020

United Nations. (1945). Charter of the United Nations, 1 UNTS XVI.

United Nations. (1970, October 24). General Assembly Resolution 2625 (XXV), UN Doc A/RES/2625(XXV).

United Nations. (2021a, July 14). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

United Nations. (2021b, March 5). Report of the 2021 Open Ended Working Group, A/75/816, Annex I.

United Nations. (2022, July 28). Open-ended working group on security of and in the use of information and communications technologies 2021–2025, A/AC.292/2022/CRP.1.

United States Department of the Army and U.S. Department of the Marine Corps Tactics and Operations Group. (2022, July). Urban operations ATP 3-06/ MCTP 12-10B. Retrieved from https://irp.fas.org/doddir/army/atp3_06.pdf

Väljataga, A. (2022, March). Cyber vigilantism in support of Ukraine: A legal analysis. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf

Wilson, A. (2017, March 15). Four types of Russian propaganda. *Aspen Review*. Retrieved from https://www.aspen.review/article/2017/four-types-of-russian-propaganda/

TO CITE THIS ARTICLE:
Svantesson, D. J. B. (2023). Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future. *Scandinavian Journal of Military Studies*, 6(1), pp. 86–101. DOI: https://doi.org/10.31374/sjms.195

Submitted: 07 January 2023
Accepted: 30 June 2023
Published: 11 July 2023