

An assessment of cyber volunteer groups in interstate conflicts and their impact on public policies

Botond Feledy^{1*}, Csaba Virág²

¹Institute of Social Reflection, Brussels, Belgium

*E-mail: b.feledy@socialreflection.org

²Nortal Cyber Resilience Center, Tallinn, Estonia

Received: 9 May 2022; Accepted: 24 May, 2022; Published online: 26 July 2022

Summary

The paper examines whether cyber volunteers are reshaping the modern conflicts. The case study serving as the proof-of-hypothesis for the paper is the Russian war against Ukraine. The hypothesis is that such groups will be part of future conflicts. We examine the conditions for group formation. We find that conditions will be present and such groups will become part of war and also of peacetime in the coming years. Hence, we advocate – *de lege ferenda* – that public policies and capabilities shall be adapted to this new reality accordingly, taking into account the capabilities, volatility and value-driven nature of these groups.

Keywords: cyber warriors, crowdsourced war fighting, cyber war, cyber space, value-based groups

Az önkéntes kibercsoportok értékelése az államközi konfliktusokban és hatásuk a közpolitikákra

Feledy Botond^{1*}, Virág Csaba²

¹Társadalmi Reflexió Intézet, Brüsszel, Belgium

²Nortal Cyber Resilience Center, Tallinn, Észtország

Összefoglalás

A tanulmány azt vizsgálja, hogy a kiberönkéntesek átforgalmazzák-e a modern konfliktusokat. A tanulmány hipotézise szerint az ilyen csoportok a jövőbeli konfliktusok szervezeti részei lesznek. E hipotézis esettanulmányát az Ukrajna elleni orosz háború szolgál. Vizsgálatra kerülnek a csoportképződés feltételei, ahol a tapasztalat azt mutatja, hogy a feltételek adottak lesznek, és az ilyen csoportok a háború, illetve a békeidő részévé válnak az elkövetkező években.

Mindez egy alulszabályozott és alulellenőrzött közegben történik. Egyrészt nincs szabályozás az államközi kibertérben sem, csupán erre való kísérletek történtek, de érdemi nemzetközi szerződés nem született. Másrészt a nemzetállami kereteken belül sem gyakori a kiberbiztonsági jogszabályok kikényszerítése, legfeljebb a gazdasági, nemi erkölcs elleni és katonai bűncselekmények esetén tudunk rendszeresen sikeres felderítésről. Jogi értelemben a kiberönkéntesek óriási kockázatot vállalnak, amely részben a saját államuk jogszabályainak valószínű megsértéséből ered, részben pedig a megtámadott ország esetleges jogi vagy egyéb megtorlásának veszélye miatt.

Ezek mellett is közel háromszázezer fős kiberönkéntes mozgalom csatlakozott az ukrán–orosz háború kibertérben zajló csatájához. Ez közel hússzor több önkéntes, mint az idegen fegyveresek létszáma az ukrán csapatok mellett. Az önkéntes csoportok megalakulásában az érték központúság játszotta a meghatározó szerepet. A háborút övező narratívák mentén karakteres ukránpárti csoportok alakultak az orosz agresszióval szemben, és reakcióként az oroszpárti csoportok létrejötte is elindult. Az ukrán kormány a kommunikációs csatornák nyitva tartásával – közös platformokon részt vesznek önkéntesek és hivatalos személyek – igyekszik rálátást, és adott esetben befolyást szerezni az önkéntesek műveletei felett.

Ez a kérdés lesz tehát a világ többi kormányzata, rendvédelme és katonasága számára feladva: hogyan lehet viszonyulni egy értékalapú csoportképződéshez a kibertérben? Érdemes ezt fenntartani és táplálni, vagy éppen ellenkezőleg, veszélyesnek tekintendők a demokráciákra, ahogy erre az NSA kiberigazgatója májusi nyilatkozatában utalt?

Ezért javasolt – de lege ferenda –, hogy a közpolitikai tervezés és szervezeti képességek ennek megfelelően legyenek igazítva az új valósághoz, figyelembe véve e csoportok képességeit, volatilitását és értékvezérelt jellegét.

Kulcsszavak: kiberháború, kibertér, értékalapú csoportképződés, magántér, közpolitika

1. Introduction

The below article is examining the effects and possible long term consequences of spontaneous bottom-up group formations in the cyber space, based on the examples of the private cyber warrior groups born in the war between Ukraine and Russia and the possible transformation effect of this on European societies.

The article is analysing how so-called cyber warrior groups – we will use interchangeably cyber volunteer and cyber partisan groups – are currently being formed based on perceived values attached to the belligerent sides in the above conflict.

If the phenomenon is here to stay with modern societies, then civilian and military public administration must prepare to accept this shift in capabilities that is potentially able to influence international relations and even outcome of a war.

At the time of the composition of the article, the war had been launched for over 60 days. The significance of the article is that the authors are introducing a new subject for research and run a systematic review of hardly existing analysis of the cyber warrior group phenomenon. The article tests the hypothesis that the formation of such groups is not specific to the current war. We examine the conditions why and how the groups are born and will draw the necessary conclusions, whether future conflicts need to take this into account.

2. Methods of inquiry

Given the very recent nature of the phenomenon, the article is based on expert interviews, report reviews and papers of relevant think-tanks. National security concerns of certain sources were taken into account. One of the authors was in direct contact with cyber warriors and relevant public groups in touch with them.

3. Observations

3.1. *The shifting border between public and private domains in assessing the phenomenon of cyber warriors*

The line between public and private domains of human activity has always been thin and mostly porous. The current developments in the war against Ukraine by Russia brought a new object for research in this regard as

the significance and the number of private cyber warriors, cyber insurgents and supporters keep growing since the start of the conflict. Private groups of skilled hackers intervened in the war in the cyber space upon the invitation of the Ukrainian government, though without the latter having any firm control over the groups. In other words, visibly private individuals grouped together to support a public and national-level (state) objective: to win a war. While current article only focuses on the cyber volunteer groups, it is important to highlight that all sorts of diverse competences and capabilities responded to the call to arms, experts from the field of defence, energy, marketing, finance, geopolitics, etc. joined with their expertise to support the cause.

The phenomenon extends to both sides of the belligerents, so pro-Russia and pro-Ukraine cyber warriors are competing with each other along, or at least parallel with the official cyber units of the two states. According to most observers and experts, the number of cyber warriors practically exceeds those being on the ground (Shore 2022). According to the currently known information and attributions, no state actor holds control – neither third states – of the ad hoc groups, therefore they act upon their own will and initiative, in communication with state services, but not depending on them. At the same time, it is important to mention that while these crowdsourced warriors are not declared state actors, there is a high chance that several state actors are actually operating under the hacktivist umbrella.

Such voluntary armies are not uncommon in the history of humankind, but certainly it is a new episode of this size in the public-private understanding of citizen-state relations (Lucas 2017). Especially that previous voluntary forces largely went under the command and control structures of the state militaries, solely the decision to join was carried out in the private domain, such is the case of the Légion Étrangère of France, voluntary drafting or mercenaries or volunteers in the Spanish Civil War or in the Finnish-Soviet War. On the other hand, private security organizations – Blackwater, Wagner Group, etc. – are in contractual relation with the state and therefore executing the will of the state with a degree of autonomy.

Historically, the private space of citizens in nation states of Western-style democracies has been growing tendentially. The private space of citizens – privacy from the state – has been born in the “salon bourgeois” according to the hypothesis of Jürgen Habermas, whereas today we witness the cyber warrior’s privacy being

born in the cyberspace (*Habermas 1962*). Actors and the regulation of their relationship in the cyber domain remains particularly fragmented and with significant loopholes due to great power misalignment in the interest (not) to regulate (*Klimburg 2017*).

Private stakeholders in war situations were so far usually focused on providing humanitarian aid and support, through donations or being near the field harbouring fugitives, wounded or those in need. Countering aggression or carrying out partisan activities was the courtesy of the citizens of the suppressed nation, usually with the monetary support and arms delivery of some external actors.

Internet, social media, the spread of competence and digitalization brought the era of ease of expressionism of support (*Clark 2012*). While so far this resulted mainly in coordination of groups, bulletins and narratives leveraging on the amplification effect provided by algorithms, the current Russian armed aggression in Europe led to the rise of active cyber insurgency, where cyber volunteers actively interfere in the warfighting state's infrastructure through cyber and kinetic attacks.

The current armed conflict called to arms a large community following a value based approach in the war that is looked at by many as clash of civilizations: the progressive and open minded nations versus the medieval imperial oppressor. This latter actually moves the activity of the current supporters beyond the hacktivism definition. Hacktivism is defined as "a form of political activism in which computer hacking skills are heavily employed against powerful commercial institutions and governments, among other targets." (*Sorell 2015*) So far hacktivist activities focused mainly on data breaches, whistleblowing and DDoS attacks supporting interests transcending particular state interests. This is the first time when a large amount of diverse global supporters actively get engaged in an armed conflict over the internet, taking targeting requests from military units or just attacking military grade targets on their own.

Currently it is still too early to state the timeline of events and their impact on each other, yet it is undisputable that the European citizens' reaction to the Russian aggression towards Ukraine forced the majority of governments to act. While governments and the EU itself tried to act as fast as it is possible the people were not that patient. Volunteers from all fields united to help Ukraine to either counter the threat or at least to mitigate the impact. While some have chosen to aid the kinetic warfare, many have chosen to support via cyber means.

3.2. Rise of the cyber partisans

On 24th February 2022, the very first day of the war, the Ukrainian government immediately called for volunteers from the Ukrainian hacker underground scene via Telegram messages for support, which it immediately re-

ceived. As Ukraine faced constant cyber attacks attributed to Russian actors, the capability already existed in the country.

The initial tasks were around espionage against Russian Forces and the protection of Ukraine's critical infrastructure. Ukrainian volunteers had been divided into offensive and defensive troops aiding Ukraine Armed Forces and Ministry of Defence in countering Russian aggression. The call was so successful that just within hours several hundreds, later several thousands of Ukrainian volunteers joined the cause. While these cyber people talented in both defensive and offensive operations were prepared for countering Russian cyber offensive operations, they were not expecting to be called to arms in reality. Along with the call to arms of Ukrainian cyber talents and professionals to defend their country from a cyber-physical threat, the world responded to the call as well: according to online sources Ukraine IT Army received the support of almost half a million people (*Shore 2022*).

Challenges rose during the process: there was no vetting. Anybody who wanted to join, joined. Some just downloaded a software provided by the IT Army to execute attacks automatically, some took a more practical approach and hacked Russian infrastructures. Managing the effort of hundreds of thousands of people is nearly impossible. In our interviews, it was recounted that professionals were trying to exploit a system, when suddenly a crowdsourced distributed denial of service (DDoS) attack executed by supporters took down the system, just to name one example.

The ghost was released from the bottle, cyber partisans, the world's hacktivist, hacker and offensive cyber capability turned against Russia. Legally speaking, it is also clear that such groups violated their own country's regulations by providing support to Ukraine with similar means. States and governments did not officially intervene with their offensive cyber capability publicly, but it seems civilian offensive capability against Russian and Belorussian targets have been greenlighted (or at least not actively hindered) as part of the global support to Ukraine and counterfeit Russian invasion. At the time of writing this article, there is an estimated amount of more than 400.000 cyber volunteers aiding Ukrainian efforts (*Shore 2022*). Although the exact number is really hard to estimate depending on who is considered to be a partisan, this is the first time in history where war fighting has gone crowdsourced and relying on global resources.

As a result, Russia's governmental and military networks, critical infrastructure providers, media, literally anything that has been connected to the internet in Russia suffered cyber attacks, data breach, or business disruptions. There are multiple reports on collapsed Russian and Belorussian networks, inaccessible systems, shut down gas pipelines and power plants, huge data leakages from large institutions and governmental organizations (*Microsoft 2022*). In Ukraine local civilians use the estab-

lished digital and cyber channels to provide information supporting local forces, documenting Russian war crimes and providing targeting information for artillery troops.

Ukraine did not develop a dedicated cyber force of its own within its military structure similar to those in Western countries or even in Russia. While the current situation generated hundreds of thousands of supporters with tens of thousands or even more of these living within Ukraine, the question already arises: what will happen to these people and to this capability once the war ends?

The incorporation of cyber operational planning into any modern and future-proof military doctrine is unavoidable, at the same time a very specific knowledge is being shared with an unvetted community for which the legal and other consequences during peace time might not be clear. The phenomenon is not only relevant from a defence capability point of view, but even more relevant from a political and policy making aspect. Value based supporters can quickly rise and pressurize governments with global support and with active intervention into digital infrastructures the amplification effect can have a significant impact.

3.3. Specific conditions for group formation

One shall make two conditions explicit about the preconditions for such cyber insurgent groups to exist. The cyber space is the very first artificial environment that humans created alone, and its rules are entirely developed by the human agency, with only indirect dependency on the natural environment, unlike all previous artificial tools and semi-environments (highway, ship, bunker, missile, agriculture, etc.). The current under-regulated state of the cyber space is the physical prerequisite of cyber insurgent group formation, supposing that the necessary digital skills and know-how is accessible to private individuals (or that they can use it in their private capacity even if trained by public bodies for public objectives). Important to mention, the bare motivation for the internet to exist has been to run communication and as such, security was not a priority at the time when the technology was defined.

Secondly, one must assess why such groups are being born. What is driving the masses of citizens with the necessary skillset to align with one or another state actor? In our hypothesis we assume that a tangible number of such groups are working out of their own will, and are not the results of covert state action, direct state influence or material benefits offered. While in the current example of the Russian aggression against Ukraine both parties are using strategic communications (stratcom) vis-a-vis their own population and third parties, we estimate that the level of intensity of those communications would not suffice alone to push for group formations.

The political science of the 21st century is describing the fragmentation of the democratic societies under several definitions, such as new tribalism (*Anzaldúa-Keat-*

ing 2009), identity politics (*Bernstein 2005*), polarization or (from a more territorial point of view) neofeudalism (*Reisman 1961*). With the accelerating speed of communication as one of the commonly accepted indicators of globalization, the group dissolution and formation in modern societies is also quicker. It means that ad hoc groups may form successfully in short time (occupy movement globally, online conspiracy groups, fringe political groups, flashmobs, or reddit's WallStreetBets, etc.) and gain unprecedented visibility in the online information space. It is one of the many driving forces behind the social polarization, visible in several Euro-Atlantic societies.

Hence, the attractiveness of value-based groups is increasing in the era of identity politics. To grow the will to fight against "an enemy" in the case of war is rather easy, as the image of the enemy is put in straightforward terms – aggressor Russia, committing war crimes against Ukrainians strategic communication (STRATCOM) versus the "nazi" Ukraine punishing ethnic Russians narrative – dividing the general population and therefore it is also mirrored in the segmentation of cyber warrior groups. The perceived values that unite each side are easy to communicate and to understand: to stand with the self-defending Ukraine and push to unite democracies against authoritarianism; while on the other side to unite against a perceived Western threat, coming in the most different forms. Important aspect to highlight is that such cyber warriors are globally recruited by the online groups. It means that globally-based individuals might decide to side with Russia just as much as pro-Ukraine hackers might decide to join from Russian or Russian controlled post-soviet territories, such as Belarus.

Several reports confirm the new fault lines of cyber warriors. "IT consulting firm Accenture describes how previous norms between hacker groups in the region are eroding and splitting groups along conflict lines. Previously refraining from conducting cyber attacks within the Commonwealth of Independent States (CIS) (a group of nine former Soviet states including Russia) the conflict has pitted hackers against one another in support of or against Russia." (*Accenture 2022; Clarke 2022: 3*) While in earlier times hacker groups mostly formed for material gains (criminality) or with some level of state support for national security objectives, one witnesses that such groups are being recently formed out of seemingly pure political alignment, based on value perception.

Group formation happened fast and seamless. Existing hacktivist and cyber criminal groups have chosen sides, especially those who are geographically located in either pro-Ukrainian or pro-Russian states. Choosing sides became almost mandatory for these groups as one of the core foundation principles of these groups is to act and not wait for the governments, or even act based on the moral commitment to a cause without any governmental

support. The US, EU, majority of the individual nation states were slower to commit to practical offensive aid to Ukraine. Offensive cyber operations do not require too much preparation compared to kinetic support. Additionally, these groups already had their offensive infrastructure, tools and tactics in place, for them it was just a matter of shifting focus on Russian targets. At the same time hundreds of thousands of individual volunteers joined the cause, representing an en masse offensive, defensive and analytic capability that needs to be coordinated to fully maximize potential (*FREE Cybersecurity & Humanitarian Services for the Ukraine War 2022; Cyber Group Tracker 2022*).

Russia and Russian Armed Forces have been hacked at an unrepresented scale, something no nation could have been prepared for. Historically nations conduct espionage campaigns against each other, targeting critical databases and infrastructures with the intention of not being detected and/or deliver destruction or disturbance at the right moment supporting political goals. This was the case with the interference in the US elections, or how cyber attacks had been carried out by Russia before the kinetic war started in Ukraine. As the pro-Ukrainian cyber community turned its focus on Russia, the result has been hundreds of millions of documents leaked, disruption in essential services like access to water, transportation, or electricity, media broadcasting pro-Ukrainian messages and access to state secrets, FSB or RAF personnel data or classified research data (*DDOS Secrets, 2020*).

While pro-Ukrainian groups have a more visible success rate, pro-Russian groups emerged as well as a response. These groups so far seem to lack both the capability to conduct operations at large against Western and Ukrainian targets and the attraction of masses. The moral and ethical values represented by the various groups seem to clearly define the opportunity to attract supporters, especially in the community with a collective memory of Soviet oppression and communist terror in Europe.

3.4. Indirect effects of the group formation

Value-based citizen communities are proliferating and redrawing the classical political fault lines of the 20th century. While classical fault lines mostly strengthen the urban–countryside division lately (abortion, same sex marriage, in vitro fertilization, democratic governance, liberal or illiberal democracy, etc.), two domains stand out as new, overarching communities. One of them is the climate change activism, the other remains the cyber domain, where cyber warriors are multi-national, multi-age and most probably different in many of their other exhibited values. In other words, these communities are issue-driven and therefore less looking for compatibility of a larger value-based identity, and more for efficiency in the chosen cause.

Further research shall be carried out to determine the profiles of larger sub-groups in the cyber partisan communities, in order to offer a more comprehensive reading of the entire community across the board. The potential for state-funded organizations (law enforcement, intelligence services, digital-focused GONGOs, etc.) to relate to the cyber warrior groups in the given country will grow in its importance. Political parties and players might try to appropriate certain platforms or groups, while others would see chaos and distance themselves from such activities.

Beyond the clearly distinguishable cyber offensive and defensive support the cyber volunteers provide, there are several groups of competences providing support for the Ukrainian government. Such as digital marketing, search engine optimization (SEO), video editing, communication and PR experts, all grouped together and ensuring the positive representation of the Ukrainian side (while defeating Russia in the STRATCOM space), hence Russia has less capability to spread its narrative outside of its own controlled channels. The coordination of these efforts, groups and individuals cannot only be described as state-of-the-art Ukrainian management skills. It is the result of co-creation process of Ukrainian defence forces and supporting cyber volunteers strengthening each other, sharing the same values and aims: leaving as less space for Russian disinformation campaigns as possible.

Soft governance approaches might be the most promising to deal with this interaction. Shared communication channels – state actors having an awareness of the operations of the groups – have worked fairly well in the Ukrainian case so far. The public organizations must remain credible in the eyes of the cyber volunteer groups, maintaining the values that the group itself is ready to work (fight) for. Given the great power game in international relations, the false flag operations and necessarily difficult strategic communications, this is not an easy task on the long term. Government changes – in a polarized social context – might be enough in themselves to turn such a group on the state, or to pacify them. Let us imagine a scenario with an alleged election interference by such a group in a democratic election process: it would have long-lasting consequences for the legitimacy of the next government, also defining a more hostile stance towards such groups.

The free-for-all cyber aspects – along with some other kinetic ones – took many by surprise and seem to be justified by the war situation. At the same time these activities can pose the problem of accountability. While kinetic war activities and actions carried out by either parties are either straightforward, claimed or at least the perpetrator is usually identifiable, this is not the case with cyber activities. Criminal and vigilant activities carried out under the cyber insurgent umbrella make it almost impossible to hold the nations accountable for the activities of the individuals inside the country.

Another risky scenario that is being weighed for the screenplays in Ukraine is when such groups commit an inadvertent escalation towards the enemy, where the state forces feel pressured to respond in a more conventional way (*Acton 2020*). In other words, a pro-Ukraine group might breach a nuclear weapons facility of the Russian Federation, which perceives it as an imminent threat and responds in kind. Practically there is no Cuban-style hotline for state actors to verify information in an instantaneous way with representatives of cyber warriors. Furthermore, one must remember that immediate attribution is nearly impossible in the cyber space, hence cyber criminals and state sponsored actors are also active in the background masquerading their actions as a supporter activity, however, serving mainly their own aims.

While the actions of the cyber volunteers have a clear impact on the current war, it is dangerous as well for the volunteers themselves. The world's cyber power has been more or less balanced for the last decade(s) among the world's leading nations. This equilibrium has been disturbed and while the impact of the support is clearly visible, it also interferes with nation state operations on both sides and civilian supporters might also become cyber targets themselves. The majority of the supporters lack proper technical and mental preparedness to ensure their own safety and security over the internet and participating in a war has its own toll on everybody. As kinetic warfighting has its dynamics and requires mental and physical preparation, so does the cyber war domain too. It seems easy and safe to enter a war from an armchair, however, we do not know what consequences the future might bring for the amateur cyber insurgent.

National Security Agency's director of cybersecurity, Robert Joyce made very critical comments about the cyber warrior involvement in the current war situation just as recently as May 2022: "You can't have the private sector influencing the doctrine between nations. (...) As you pointed out, it's illegal. But it's also unhelpful, because one of the things we talked about is we're trying to get Russia to take account for the ransomware attacks and hacks that come out of Russia and emanate." (*Demarest 2022*) The tone of the speech shows the level of concern inside one of the largest actors of the US cyber landscape.

To demonstrate the challenges posed by the sheer presence of such groups, let us examine another hypothesis, where the cyber warrior group gets penetrated by the enemy forces. The size and social dynamic of the groups would make them a rather easy target for a similar operation that plants a foreign agent inside. In this case, a false flag operation could be produced (by pushing the group into an inadvertent escalation that gives the pretext for the other side to act), or leaks could get falsified to offer venues for counternarratives. This is already visible as Russian Armed Forces are checking captured Ukrainian citizens, mobiles for Ukrainian IT Army software and messages in the so called "filtration camps"

or spreading weaponized software packages targeting volunteers.

Finally, there is the risk of the volunteer cyber insurgents to use their freshly gained knowledge and capability to turn their activities profitable. While we assume the majority of the supporters are not criminal minded, even if a smaller amount of cyber war veterans turn towards the cyber criminal world they can present a significant capability. These people or smaller groups are experienced, have an understanding of tools and tactics and potentially know how not to get caught. Their skills and background make them highly attractive for both the ethical hacking and intelligence community along with the criminal underground.

So public administrations and intelligence services both need to adapt to the new realities of cross-border, multinational, thematic-focused, value-based groups acting alone on the international scene. The governmental community has to be prepared that status quos can be disrupted from one moment to another and instead of fighting it, they need to adapt to the changing landscape and leverage on that. This requires technical, social, cultural and many other competencies converged into governmental capabilities, that many governmental organizations are not yet prepared to implement.

4. Conclusions

The observed new phenomena – both in the cyber space and in climate change activities – are driving to a renewed social contract between the state and its citizens. The century old mandates that traditionally European sovereign states took on are facing serious challenges. In some cases, the mandate seems to expire and needs to be reconsidered for more subsidiarity, leaving it to the citizens to decide instead of national level regulations; while other loopholes are wide open and citizens are unprotected, such as in the case of certain cyber threats, data protection and cyber war.

Resilience to cyber threats requires and presupposes an excellent cooperation between private and public actors, with live channels of communications being open 24/7, even in cases where the private actors are simply a conglomerate of active citizens without further organization. Cyber operational planning both in the defence and governmental domains have to be incorporated into everyday practices along with the analytic capability generating actionable intelligence for stakeholders.

Given the examination of the conditions how cyber volunteer groups are created in conflicts in the 21st century, we take our hypothesis corroborated and accept that such groups will remain natural elements of future conflicts and their participation (or hostility) could influence interstate relations. Therefore, we advocate for the revisit of military doctrines, cyber war planning and for the reassessment of the value-driven foreign policy strategic communication.

Regarding the potential for online phenomena to impact human lives outside of the cyber space – offline – the policy makers need to be particularly attentive to how best to draft a soft approach to this new relationship. Stratcom – friendly and hostile – can cause a sudden change to the momentum (attractivity, dynamics and retainment rate) of the volunteer groups. Stratcom planning must be conscious about this aspect. Government communication and actions might be vetted more often by such groups whether they reflect the values of the group.

The long-term repercussions of the cyber volunteers en masse need to be studied and incorporated into policy planning as quickly as possible.

References

- Accenture (2022) Global incident report: Threat actors divide along ideological lines over the Russia-Ukraine conflict on underground forums. Accenture Report, 14 March 2022. <https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf> [Downloaded: 5 May 2022].
- Acton, J. M. (2020) Cyber warfare & inadvertent escalation. *Daedalus*, Vol. 149. No. 2. pp. 133–149. https://doi.org/10.1162/daed_a_01794
- Anzaldúa, G., & Keating, A. (2009) *The Gloria Anzaldúa reader*. Durham & London, Duke University Press.
- Bernstein, M. (2005) Identity politics in annual review of sociology. *Annual Reviews*, Vol. 31. pp. 47–74.
- Clark, E. (2012) Social media is our media. <https://www.diva-portal.org/smash/get/diva2:539573/FULLTEXT02.pdf> [Downloaded: 7 May 2022].
- Clarke, A. (2022) *Hacking the invasion: The cyber implications of Russia's invasion of Ukraine*. Thirdway Publication. <http://thirdway.imgix.net/pdfs/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine.pdf> (p. 3).
- Cyber Group Tracker (2022) <https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-6e08ef31c533> [Downloaded: 1 May 2022].
- Demarest, C. (2022) NSA cyber boss seeks to discourage vigilante hacking against Russia. *C4ISRNET*, 5 May 2022. <https://www.c4isrnet.com/cyber/2022/05/05/nsa-cyber-boss-seeks-to-discourage-vigilante-hacking-against-russia/> [Downloaded: 9 May 2022].
- DDOS Secrets (2020) Category: Russia. <https://ddosecrets.com/wiki/Category:Russia> (Last edited: 21 November 2021) [Downloaded: 5 May 2022].
- FREE Cybersecurity & Humanitarian Services for the Ukraine War (Est. 24 Feb 2022) https://docs.google.com/spreadsheets/d/18WYY9p1_DLwB6dnXoiiOAoWYD8X0voXtoDl_ZQzjzUQ/edit#gid=0 [Downloaded: 9 May 2022].
- Habermas, J. (1962) *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Frankfurt a. M., Suhrkamp.
- Klimburg, A. (2017) *The darkening web: The war for cyberspace*. New York, Penguin Press.
- Lucas, G. (2017) *Ethics and cyber warfare. The quest for responsible security in the age of digital warfare*. Oxford, Oxford University Press.
- Microsoft (2022) Microsoft's special report on Ukraine, 27 April 2022. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> [Downloaded: 20 May 2022].
- Reisman, G. (1961) *The revolt against affluence: Galbraiths Neo-Feudalism*. New York, The Objectivist, Inc.
- Shore, J. (2022) Don't underestimate Ukraine's volunteer hackers. <https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/> [Downloaded: 5 May 2022].
- Sorell, T. (2015) Human rights and hacktivism: The cases of Wikileaks and Anonymous. *Journal of Human Rights Practice*, Vol. 7. No. 3. pp. 391–410. <https://doi.org/10.1093/jhuman/huv012>.