INTERNATIONAL CONFERENCE RCIC'22
Redefining Community in Intercultural Context
Braşov, 5-7 May 2022

SOLVING AND MANAGING MORAL DILEMMAS. FROM THE CYBER BATTLE FIELD TO THE FUTURE OF MANKIND

Ella-Magdalena CIUPERCĂ*, Victor Adrian VEVERA**

* Cyber Security and Critical Infrastructure Department, National Institute for Research & Development in Informatics, Bucharest, Romania, ** General Director, National Institute for Research & Development in Informatics, Bucharest, Romania

Abstract: *The way individuals make choices when faced with moral dilemmas defines them, gives them coherence, authenticity, and contributes to their self-image. When they are attracted to opposite and incompatible directions, people make choices that are predominantly dependent on irrational elements and, very rarely, rationality becomes a working criterion. Morality, principles of conduct, truth, fairness can take on different connotations depending on the pressures of the situation. Traditional examples of professions that often face moral dilemmas are soldiers or intelligence officers. In this paper, we aim to detail the specifics of a new profession, which puts skills of the future in the service of crime or of the community good, weather in time of peace or war, analyzing the dyad hacking/ethical hacking. We will use the Anonymous Group as a case study, an ideology with a specific specificity, which in the context of the Russian - Ukrainian war can turn into a community resource or may turn hacktivism into a source of future anarchism in society.*

Keywords*: hacktivism; ethical hacking; cyber battlefield*

1. INTRODUCTION

One of the most important elements that we need to be aware of is that every social change is accompanied by important changes in the social norms that govern the behavior of the community, and the moral values associated with them. Social activists have proven to be a key factor in generating socio-political change (Arquilla & Ronfeldt, 2001, Ganesh& Zoller, 2012; Shragge, E., 2013), and contemporary reality offers us many examples of civic activism that needs to be closely monitored (Vevera & Ciupercă, 2019). In order to bring about the desired change, groups of social activists identify certain components of society that they consider inappropriate for the society of the future and that they will constantly attack.

Understanding how social activists are able to set the moral and ethical agenda of society can only be achieved if the way in which the main social institutions caught up in the roller coaster of change are understood. People behave in different ways because in the background act a series of values and rules that have been promoted by certain social institutions and adopted by individuals. Therefore, every time society undergoes important changes, transformation nullifies a source of society's ethics and morals. The more authoritative and inflexible this source is, the more affected and at risk of extinction it is (Jordan & Taylor, 2004).

2. SOCIAL CHANGE IN THE CROSSROADS OF SOCIAL ACTIVISM

Social activism as a source of social change needs to be properly understood so that its patterns of manifestation are quickly recognized and the effects anticipated. History has shown that social activism determined the future direction of the evolution of societies, whether progressive or destructive: The Bolshevik Revolution was a regressive factor, while the abolition of slavery was a huge step in social history. Political conflicts and social turmoil have been specific to all the great changes that society has undergone, creating the framework for social participation, the emergence of social movements and popular political activism.

Activist networks have generated protests, social movements, but also new forms of ethics and morality, moved social norms to spheres less explored by the majority, questioning the actions of most members of society.

The behavior and effects of these groups have long attracted the attention of experts in many fields who have sought to understand how they work and the mechanisms by which they manage to change the course of history - while political science has studied them from the perspective of the way they generate new forms of socio-political organization or even anarchy, sociology has been interested in how they propose new social norms, and social psychology has studied them as active minorities being focused on the intrinsic mechanisms of this paradoxical process in which people without significant resources of social capital, money, prestige or any other power can innovate (Moscovici & Faucheux, 1972; Maass & Clark, 1984). Examples of past activism are numerous - from Christianity, to animal rights, environmentalism, feminism, progressivism are just a few examples that have changed the course of social history.

The study of social activism groups highlighted some common dimensions of their behavior (Jordan & Taylor, 2004):

- they PROPOSE NEW FORMS OF SOCIAL ETHICS, of social justice, which will guide the future functioning of society;
- they are in a HURRY - they want to bring about social change quickly, without any delay;
- they propose NON-FAMILIAR models of future societies, which involved TRANSGRESSION from the normal lifestyle to an unusual one;
- they are UNITED and people feel that they belong to these groups with which they identify;
- they are CONSISTENT in denigrating what is considered bad and intend to change;
- they manifest itself directly, VISIBLE against an item of the society considered to be wrong, which they want to change.

The relationship between democracy and activism has embraced a winding path over time, as activist movements in the physical or online environment have rather authoritarian characteristics and may promote social change that contains the germs of anarchy.

3. ONLINE SOCIAL ACTIVISM AND HACKTIVISM

Today, the new social structures are characterized by revolutionary communications, new patterns of family association, transnational production lines, new types of spiritual communities, all united in a simplistic name – the information society. With the emergence of a new environment for the manifestation of human daily activities, namely the cybernetic one, a new dimension for manifestation of socio-political activism has become available. When the activity of the questioned institutions is essentially characterized by the cyber compromise in the name of an ideology, we deal with a new type of online social activism – hacktivism, often considered the main way to fight in the digital space (Wray, 1998).

Online social activism should not be confused with hacktivism. The first refers to the use of the Internet and digital space to support causes or ideals especially by creating websites, posting materials, identifying information, sending emails, setting up forums, forming associations, without disturbing in any way the activities of other users. In contrast, hacktivism consists of operations that use the same techniques that hackers use to cause malfunctions of the normal operation of some sites, still without causing serious damage. It can be said that hacktivism is politically motivated hacking. Failure to comply with this criterion and involvement in operations that end in significant costs to the other party, including material and / or human damage, go beyond the specific area of hacktivism and place those operations in the category of cyberterrorism (Scott & Cupp, 2017).

The infusion of social activism into the digital space has reinvented hacking. Until the advent of hacktivism, hacking was rightly considered an activity to hardly avoid, with significant deviations from ethics and morals. Public perceptions of hackers were improved when they assumed higher motivations and engaged in illegal clandestine activities in the service of a common good and seemingly progressive ideologies (Hampson, 2012, McNutt, 2018).

Hacktivism is currently in a gray area between protesting against things going wrong in society and illegal activity, with involved people being labeled as freedom fighters or as a group that pursues the digital lynching of chosen targets. Therefore, although hacking is rightly perceived as a type of theft and is associated with illegal, criminal activities, hacktivism (sometimes called electronic civil disobedience, Wray, 1998) is considered only another form of protest, being totally acceptable to the proponents of the idea in favor of which it is protested.

As daily activities move into the digital space, hacking and hacktivism become more and more prominent. Today's hacktivism tends to cling to the spirit of the times and to assume the support of progressive causes of the time - for example, digitally correct hacktivism.

The profile of the activists involved in social activism and hacktivism is a difference between these types of protest that should be considered more often.

In the case of those who advocate for a social change in the physical world, the identity of the protesters is known, and those people generally have no criminal record. Hacktivism is, however, carried out by anonymous people, people who probably have previously performed activities of decryption, violation of privacy, access for personal financial gain, not for a political stake. Therefore, the accumulation of high social and trust capital by people with dangerous social values and questionable psycho-moral traits, the social change may be triggered to change to undesirable directions as soon as they may become opinion leaders

4. HACKTIVIST GROUPS IN THE RUSSIAN-UKRAINE CONFLICT

What role does the Internet play in foreign policy decisions and in international developments? It seems that it is more and more extensive as the examples do not stop to prove it. In April 1999, according to the Los Angeles Times, the Kosovo war of 1996-1999

> turned cyberspace into an ethereal war zone where the battle for hearts and minds is being waged through the use of electronic images, online discussion group postings and hacking attacks (Dunn, 1999, 10).

The conflict in Kosovo was considered the first war on the Internet, this space being used for disseminating propaganda, asking for help, demonizing the opposing camp. After that, the war acquired new dimensions, overcoming traditional ideological justifications and no longer confining itself to military power (Lesenciuc, 2007), but encompassing new fields for battle.

At the other end of the time continuum, with the invasion of Ukraine by Russia, the digital space was divided again between the followers of the two camps. The visibility of the Ukrainian conflict has attracted hundreds of hackers, volunteers from all over the world. The possibilities given by technology and their localization around the globe make it almost impossible to identify the perpetrators of the various attacks that take place subsumed by this conflagration - the hybrid war and especially the cybernetic war has reached a peak hard to imagine before.

Aware of the precariousness of the way in which this huge resource is exploited, the Ukrainian authorities have initiated several actions to centralize and direct the efforts of volunteers. In the early days of the conflict, the Ukrainian government knew how to seize the opportunity and announced, through the voice of Ukrainian Deputy Prime Minister Mykhailo Fedorov, the establishment of an IT Army to help countering Russian attacks by denying access to cyberspace. Through a Twitter ad, he channeled volunteers to a Telegram channel with precise directions that could be followed by volunteers to contribute to a more complex overall puzzle of defense and attack A 14-page document detailed specific instructions - what software to use, how to hide their identity. Targets were posted every day, targeting mainly telecommunications companies, banks, ATMs. In about one week, the channel had 285,000 subscribers. The co-founder of the Ukrainian cyber security company Cyber Unit Technologies, Yegor Aushev, has called on programmers to get involved in the conflict and offered $ 100,000 for those who identify flaws in the code of Russian cyber targets. To be accepted each participant should have someone else's recommendation to be accepted.

The involved hackers have mostly used DDoS attacks, in which a server is overwhelmed by a wave of requests. These are relatively easy to do and only temporarily disconnect websites. The most salient hacktivist groups in the Russian – Ukrainian conflict are by now (blog.checkpoint. com/2022/03/03):

- **AgainstTheWest** is an active hacktivist group since October 2021, which used to attack entities suspected of having links with the Chinese Communist Party before the war. On February 13, 2022, they decided to dissolve due to lack of motivation, but they met again because the war and announced that they would collaborate with Anonymous against Russia.

- **KelvinSecurity** labeled itself as Private Information Hacker Company. On March 1, the group published a link that lead to the "monitoring system of the Nuclear Reactor in Dubna", a "leaked database from the Russian nuclear institute" and the "video from nuclear reactor". However, with the exception of some Twitter messages, there is no other evidence that the group really managed to penetrate the Nuclear Reactor at the Joint Institute for Nuclear Research in Russia.

NB65, which works also in support of Ukraine, "declared a successful campaign against ... The Institute of Nuclear Security [in Moscow] and published sensitive documents", according to the report of the cyber security company CyberInt.

Cyberpartizan, a group of cyber activists in Belarus who oppose President Lukashenko, said they control the national railway system and will sabotage any trains carrying members of the Russian army and they have encrypted and / or destroyed databases that allow control of traffic, customs, stations in Belarus (https://www.
theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup).

Also in Georgia, the BlackHawk group has launched attacks on Russian bank servers and TV channels.

KillNet, which operates in support of Russia, has launched a "KillNet Botnet DDoS" service and is running campaigns against Anonymous, which have announced support for Ukraine. On March 1, they announced that they had managed to compromise the Anonymous website, as well as retaliation for attacks on Russian sites.

Anonymous. Beyond these examples, Anonymous is probably the most well-known hacktivist network in the world. Formed in 2003 as a decentralized hacktivist group, united under the motto "We are a legion", Anonymous operates in an atypical manner, in the sense that anyone can adopt a cause and act in its support, under the auspices of Anonymous, provided that the attacks be directed against an organization that misuses its power. The symbol with which they became famous is the Guy Fawkes mask, made famous by Alan Moore V's graphic novel for Vendetta, in which an anarchist revolutionary overthrows a corrupt fascist government. They gained the most visibility between 2008 and 2014, following cyber-attacks against entities such as the Church of Scientology and PayPal. Anonymous has previously hit Isis, the Iraqi terrorist group and the Ku Klux Klan, as well as payment companies, local governments and the record industry. Some attacks have led to the arrest of members by US and UK authorities. Currently, the group has numerous social media accounts, with 15.5 million following only on Twitter pages.

Following the Russian invasion of Ukraine, the group focused on attacking the vehicles of Russian disinformation campaigns, such as media agencies, as well as hacking funds from certain Russian financial institutions to donate them in cryptocurrencies to Ukrainian efforts.

A resounding achievement was the takeover of the Russian television channel, which in its program replaced Russian propaganda with images depicting the horrors of the war in Ukraine and the atrocities committed by the Russian army. In a short video, a regular program of Russian television was interrupted by images of bombs exploding in Ukraine and soldiers talking about the horrors of the conflict. The video appeared on the third day of the war, on February 26, and was widely circulated on social media.

Anonymous also claimed a distributed denial of service attack against the Russian news agency Rostelecom, although it never commented on the veracity of the allegation. They also managed to change the international maritime records in which they changed the name of Putin's yacht in the FCKPTN to which they described the destination HELL and showed that he was shipwrecked on Snake Island, recognized as a symbol of Ukrainian resistance. The websites of the Moscow Stock Exchange, Russia's federal security agency and the country's largest bank, Sberbank, have been temporarily shut down.

Numerous independent groups were attracted under the auspices of Anonymous, an example of this being **Squad 303**, a group of Polish hacktivists who borrowed the name of a Polish fighting squadron, famous in the Second World War. They have built a website that allows everyone to send SMS and WhatsApp messages to random phone numbers in Russia where they can tell the truth about the war in Ukraine.

The public's involvement in this type of confrontation also has the disadvantage that it gives the opposing camp the opportunity to strike them with its own weapons.

> The Achilles heel of Anonymous is that anyone can claim to be Anonymous, including state actors operating against what we're fighting for. With our current rise in popularity, it's (almost) a given that there will be obvious repercussions from a government entity. As for adding to the chaos, we're used to chaos, especially online (Anon2World, *apud* https://www.bbc.com/news/ technology-60784526).

5. COSTS AND BENEFITS OF HACKTIVISTS INVOLVEMENT IN INTERNATIONAL CRISIS

The discussion on the risks and benefits of involving hacktivists in an international conflict is broad and should be carried out on short term and long term level.

a. Short term. The attacks carried out by anti-Russian groups manage to disrupt the functioning of some sites, to promote pro-Ukrainian or anti-Russian messages, where censorship would not allow them or even to take embarrassing actions for the authorities involved in the conflict. For example, the supply of electric vehicles on the Moscow - St. Petersburg highway was suspended for a day by the Russian energy company Rosseti, because the terminals displayed the message: "Putin is a dickhead". Sometimes it happens that announcements about the compromise of cyber security of certain institutions considered adverse tend not to be confirmed.

On the other hand, experts warn that these cyber guerrilla efforts could enter unexplored territory: "If one of these activists, one of these volunteers, comes

across something and someone dies, then the first shot is fired," said Mike Hamilton, former Vice President of the US National Services Coordinating Board and Chief Information Security Officer of the cyber security firm Critical Insight. Thus, instead of helping to shorten the conflict, there is a risk that hacktivism will lead it to a larger scale.

"It's become an independent machine, a distributed international digital army" (Aushev, 2022). Experts already warn of the impossibility of controlling this type of fighting force

> It is crazy, it is bonkers, it is unprecedented. This is not going to be solely a conflict among nations. There are going to be participants that are not under the strict control of any government (Matt Olney, 2022).

In the absence of any control and even motivated by good intentions, these volunteers could accidentally damage critical infrastructure such as hospitals or communications.

> I've never seen anything like this. These attacks do carry risks. [They] could lead to escalation, or someone could accidentally cause real damage to a critical part of civilian life.

says Emily Taylor from the *Cyber Policy Journal*.

The risks seem to be getting bigger than the benefits every day, especially since the effects produced by hacktivists are not very impressive. The benefits of anonymity and relocation can turn into huge risks at the moment Russia decides to adopt a foreign flag and get involved in cyber-attacks behind a hacktivist identity.

Security experts believe that poor results are especially because of a lack of specialized training in cyber warfare. Due to their lack of military training, assumed coordination and a well-established global plan, the damage they do is not great enough to reverse the fate of the war or at least cause insemination damage. "The land invasion is advancing, people are suffering, buildings are being destroyed. Cyberattacks can't realistically impact this." (Lukasz Olejnik, https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html).

The question is whether hacktivists can't or don't want to do more damage? Our hypothesis is that, in fact, hackers subscribe to the classic definition of hacktivism, their main characteristic being the production of damage, but not an irreparable one, just temporary. Voluntary hackers seem to avoid becoming cyberterrorists, probably due to the fact that they do not have a soldier's education, trained to destroy their target. According to their profile they are rather willing to cause material damage and momentary dysfunctions, not serious permanent ones.

b. Long-term. On the other hand, an unexpected result of this war is the fact that it united under the same banner entities in total opposition: the social activists and those against whom they traditionally fought – the state authorities. The hackers had previously participated in the war in Syria, but in such small numbers that it was insignificant, but the war in Ukraine has turned this behavior into a social phenomenon whose future evolution is a big question mark.

We are therefore facing a paradigm shift that requires special attention, not only for its immediate effects, but also because of the possible long-term consequences. The evolution of events must be carefully monitored, both in terms of the characteristics of the situations currently experienced, and in terms of the social capital obtained by hacktivists and the skills developed by them during the conflict.

Scenarios for the evolution of situations should be built permanently both for the war period, but especially for post-war context with the scope of rising the resilience of people and critical infrastructure (Barbu, 2016). How will the tools learned today be used and for whose purposes could they be enslaved? From our point of view, this is a crucial question for the construction of plans for rapid reaction measures for future situations that we will face in the Russian-Ukrainian post-conflict scenarios. In the absence of such concerns, which should be reflected in careful and swift response, we fear that things will turn into an undesirable directive, and that the social order could be affected in the long run.

In fact, Ukraine seems to understand the risks associated with the opening of a Pandora's Box as Victor Zhora, a senior cyber security official at the State Service for Special Communications and Information Protection in Ukraine, said that although they did not welcome "any illegal activity in cyber space" he "understands" and "appreciate" what Anonymous and other hacktivists are doing.

> The world order has changed ... and I don't think sticking to moral principles works since our enemy doesn't have any principles. We appreciate every kind of help. (*apud* Murphy, 2022).

6. CONCLUSIONS

The Russian-Ukrainian conflict is probably the most important of those who have used cyberspace as a means of full-fledged operational battle field. Hacktivists may become a constant in future wars. But the features discussed above require increased attention from decision makers, even after the end of the conflict. Reality has shown that the level of volunteering in such situations is much higher, compared to other forms of people involvement in the conflict, even for the simple fact that the conservation instinct acts to a lesser extent and no real threats are perceived for those who want to involve. Still the disorganization of a large number of relocated volunteers can have undesirable effects and can even become a danger to the evolution of the conflict and, especially, to peace negotiations. Therefore, although a first reaction to these actions may be to approve and support, the long-term consequences of these actions should not be ignored. IT, military, political, and diplomatic experts gathered in dedicated working groups should consider each type of action and its potential long-term effects to enable feedback on the needs of the community, which would be ideal based on clear documents and regulations, currently non-existent.

In this article we have tried to suggest the scale of the problem by describing the activities carried out in support of Ukraine, in order to understand that the approval for war hacktivists could degenerate later. The right reaction of decision makers is to channel these energies in a desired and socially useful direction during the war but especially afterwards. The lack of concern for regulation will create the right framework for some anarchist activities fueled by hacktivist groups that have reached their highest potential during previous conflicts.

7. ACKNOWLEDGMENTS

This work was funded from the project "Cybernetic polygon for industrial control systems (ROCYRAN)" ("Poligon cibernetic pentru sisteme de control industrial (ROCYRAN)").

The authors take full responsibility for the contents and scientific correctness of the paper. The selections of the texts to include depend on the result of the peer review process announced.

BIBLIOGRAPHY

1. Arquilla, J. & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: Rand Corporation.
2. Barbu, D.C. (2016). Îmbunătăţirea protecţiei infrastructurilor critice din sectorul TIC prin creşterea rezilienţei. *Revista Română de Informatică şi Automatică*. No 4.
3. Denning, D.E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In John Arquilla & David Ronfeldt (eds.), *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: Rand Corporation. 239-288.
4. Dunn, Ashley. (1999). Crisis in Yugoslavia –Battle Spilling Over Onto the Internet. *Los Angeles Times*, 3 April 1999, sec.A, p.10.
5. Ganesh, S. & Zoller, H. M. (2012). Dialogue, activism, and democratic social change. *Communication Theory*. 22(1). 66-91.
6. Hampson, N.C. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review*. 35 (2). 511-542.
7. Conger, Kate & Satariano, Adam. (2022, 4 March). Volunteer Hackers Converge on Ukraine Conflict With No One in Charge. *The New York Times* [online]. Available: https:// www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html [Accessed March, 2022].
8. Jordan, T. & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge.
9. Lesenciuc, A. (2007). The End of Ideologies and the Military Power.*Review of the Air Force Academy*. (1). 77-80.
10. Maass, A. & Clark, R.D. (1984). Hidden impact of minorities: Fifteen years of minority influence research. *Psychological Bulletin*. 95(3). 428-450.
11. McNutt, J.G. (Ed.). (2018). *Technology, activism, and social justice in a digital age*. Oxford: Oxford University Press.
12. Moscovici, S. & Faucheux, C. (1972). Social influence, conformity bias, and the study of active minorities. In *Advances in experimental social psychology*. Vol. 6. Cambridge, MA: Academic Press. 149-202.
13. Murphy, Hannah. (2022, 4 March). Ukraine war sparks revival of hacktivism. *Financial Times* [online]. Available: https://www.ft.com/ content/9ea0dccf-8983-4740-8e8d-82c0213512d4 [Accessed March, 2022].
14. Roth, Andrew. (2022, 25 Jan). 'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup. *The Guardian* [online]. Available: https://www.theguardian. com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup [Accessed March, 2022].
15. Scott, T.W. & Cupp, O.S. (2017). The Ethics of Hacktivism. In *The Ethics of Future Warfare*. Special Report. Fort Leavenworth, Kansas: Lewis and Clark Center. 143-148.

16. Shragge, E. (2013). *Activism and social change: Lessons for community organizing*. Toronto: University of Toronto Press.
17. Tidy, Joe. (2022, 20 March). Anonymous: How hackers are trying to undermine Putin. *BBC News* [online]. Available: https://www.bbc.com/news/technology-60784526 [Accessed March, 2022].
18. Vevera, A. V., & Ciupercă, E. M. (2019). The dimensions of cyber warfare in the sino-russian space. *Romanian Cyber Security Journal.* Fall 2019, vol.1, no.2. 31-36.
19. Wray, S. (1998). Electronic civil disobedience and the World Wide Web of hacktivism Paper presented at the *Socialist Scholars Conference*, New York, New York, March 20-22.
20. ***. (2022, 4 March). Hacktivism in the Russia-Ukraina War, Questionable Claims and Credit War. *Check Point* [online]. Available: https://blog.checkpoint.com/2022/03/03/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/ [Accessed March, 2022].