Anonymous Hacktivism: Flying the Flag of Feminist Ethics for the Ukraine IT Army[1]

Ellen Cornelius, J.D.
J.D.| The Center for Health & Homeland Security

In January 2022, Russia began its assault. Russian forces launched wiper malware against Ukraine's Foreign Ministry and networks used by the cabinet.[2] Russia launched several attacks such as Distributed Denial-of-Service (DDoS) attacks against Ukrainian banking and defense websites in early February, and again, Russia launched wiper malware against Ukrainian government systems on February 24th.[3] Further, Russia launched its ground invasion against Ukraine on February 24, 2022.

> ***Women are intimately involved in Russia's war on Ukraine and are permitted to serve in combat roles in the military.***[5]

Throughout history, in both the military world and the hacker world, the male gender has been predominant. Feminist ethicists aim to understand, criticize, and correct: (1) the binary view of gender, (2) the privilege historically available to men, and/or (3) the ways that views about gender maintain oppressive social orders or practices that harm others, especially girls and women who historically have been subordinated, along gendered dimensions, including with respect to sexuality and gender-identity.[4] Women are intimately involved in Russia's war on Ukraine and are permitted to serve in combat roles in the military.[5] Even though the numbers are low and the historical privilege remains with men, women serve as elected officials in Ukraine. Women currently comprise about 20% of the Ukrainian parliament.[6]

However, Ukraine's voluntary IT Army has turned hacking into hacktivism, which means that hacking is aimed at political goals.[7] Therefore, women and non-binary people's hacktivism during the Russian attack on Ukraine may lead to the fullest participation in cyber activities and politics that we have ever seen in Ukraine.

Russia's attacks on Ukraine are not unique to 2022. From 1853-1856, Russia fought the Ottoman Empire in the Crimean Wars. Russia did not take over Crimea in the 19th century; however, it invaded again in 2014. Russia has occupied Crimea since 2014. In the first "full scale battle in which traditional and cyberweapons have been used side by side"[8] Russia invaded Ukraine on Thursday, February 24, 2022.[9] The dual nature of Russia's war on Ukraine has countless consequences. "In many instances, Russia coordinated its use of cyberweapons with conventional attacks, including taking down the computer network of a nuclear power plant before moving in its troops to take it over."[10] Infrastructure is a high value target. "Satellite internet provider Viasat was hit by a cyberattack which caused wide-ranging communications outages throughout Ukraine on February 24."[11]

Aushev asked volunteers to aid in protecting Ukraine's critical infrastructure and conduct digital espionage operations on invading forces at the behest of the Defense Ministry.[14]

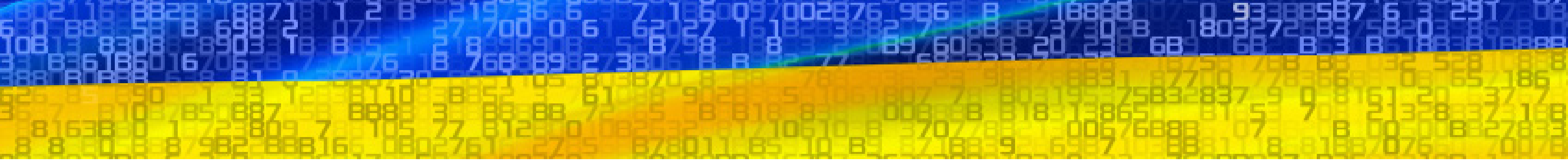
Prior to the Russian invasion on February 24th, the IT industry and tech startups had been flourishing in Ukraine. However, there was no cybersecurity force in the Ukrainian military that was solely devoted to offensive or defensive operations.[12] Nonetheless, since Russia's occupation of Crimea in 2014 through the present time, information security has been increasing in importance. Yegor Aushev, co-founder of Cyber Unit Technologies in Kyiv, issued a request for help on the 24th of February.[13] Aushev asked volunteers to aid in protecting Ukraine's critical infrastructure and conduct digital espionage operations on invading forces at the behest of the Defense Ministry.[14] Volunteers were vetted and they were asked to include their specialties and references on their application.[15] "Volunteers were asked how many years' experience they have in 12 specific areas, ranging from open source intelligence gathering and social engineering to malware development and DDoS operations. Those signing up were also asked to provide the name of a trusted reference who could vouch for their credibility."[16] The Ukrainian government is part of this mission. "The IT Army has had a relatively public presence since last weekend when Mykhailo Fedorov, a Ukrainian deputy prime minister in charge of digital transition, made a public appeal to Ukraine's tech workers to join a Telegram channel called the "IT Army of Ukraine," which had more than 280,000 subscribers as of Friday."[17] A volunteer unit — led by the Ukrainian government during war – has been characterized as an innovative development.[18]

Ukraine's IT Army is on the offensive and acting out of self-defense as well. "Beyond striking back at Moscow, Aushev said his team would help Ukraine's military hunt down undercover Russian units invading cities and towns. He said his group had discovered a way to use cellphone tracking technology to identify and locate undercover Russian military units moving through the country, but declined to provide details."[19] Volunteers are explicitly aiding the military. "The IT Army will likely take on defensive tasks to free up Ukraine's government hackers."[20] The number of unpaid workers has created an advantage for Ukraine. "And what some officials believe here in the U.S. is that what's happening is because the Russian hacking teams are having to defend so much, it's sort of making it harder for them to do any sort of offensive operations against Ukraine that they might have otherwise planned to do."[21]

In addition to tracking and playing defense, the volunteers are launching attacks as well. On February 26, 2022, Ukrainian Vice Prime Minister called on the IT Army to take down 31 Russian government, banking, and corporate websites.[22] DDoS attacks have continued to be successful. "The channel's administrators, for instance, asked subscribers to launch Distributed Denial of Service attacks against more than 25 Russian websites. These included Russian infrastructure businesses, such as energy giant Gazprom, the country's banks, and official government websites. Websites belonging to the Russian Ministry of Defense, the Kremlin, and communications regulator Roskamnadzor were also listed as potential targets. Russian news websites followed."[23] Ukraine has benefited from these disruptions and distractions. "The IT Army targeted the websites of several Russian banks, the Russian power grid and railway system, and have launched widespread DDoS attacks against other targets of strategic importance. The bulk of Ukrainian cyberpower appears to be stemming from the IT Army."[24] The IT Army has been a valuable addition to Ukraine's wartime efforts by attacking Russian infrastructure. In addition to DDoS attacks, the IT Army has countered Russia's misinformation campaign.

Historically, Russia's playbook includes misleading information, and the war against Ukraine is no different. "As Russia continues to spread misinformation about the purpose of its presence in Ukraine, leaks along these lines could be a powerful antidote, undermining domestic support for the war and providing a basis for other countries to hold Russia accountable for its diplomatic and military actions. In addition, DDoS attacks may affect public opinion in Russia. A steady stream of inconveniences and disruptions will likely increase Russians' discontent with the war."[25] The IT Army is devoting its time and resources to dispelling the myth that Ukraine is committing genocide against Russians in the Donbas region. "Perhaps the most significant impact the hacktivists could have is damaging Russia's reputation both domestically and internationally as well as undermining its misinformation narratives by leaking data from Russian organizations."[26]

While the IT Army has been effective, Russia's cyber forces have been able to perpetrate attacks. Russia launched DDoS attacks in early February 2022 on banking and defense websites.[27] Not all of Russia's attacks have been successful. "Moscow conducted more cyberattacks than was realized at the time to bolster its invasion, but more than two-thirds of them failed."[28] There are many reasons for the failures. "But many of the attacks were thwarted, or there was enough redundancy built into the Ukrainian networks that the efforts did little damage. The result, Mr. Smith said, is that the attacks have been underreported."[29] Help came from outside Ukraine as well. "It indicated that Ukraine was well prepared to fend off cyberattacks, after having endured them for many years. That was at least in part because of a well-established system of warnings from private-sector companies, including Microsoft and Google, and preparations that included moving much of Ukraine's most important systems to the cloud, onto servers outside Ukraine."[30] As the war grinds on, this unique partnership is likely to be beneficial to Ukraine.



> ***In cyberspace, it is possible for women and non-binary people to function without the historical negative consequences that are attached to their gender.***

The IT Army has been an unusual addition to the Ukrainian military's response to Russian attacks. Hacktivists are being recruited based on their specialties. Hacking has been dominated by men for many years.[31] Women are hackers; however, many women are harassed when their gender is revealed online.[32] Similarly, the military continues to have its top ranks filled by a majority of men. Men maintain these two systems, but hacktivism during war may change things.

In cyberspace, it is possible for women and non-binary people to function without the historical negative consequences that are attached to their gender. "Fortunately, the few women who break through to the "elite" ranks of hacking find that at the top, what matters is your technical skills, not your gender."[33] At the lower ranks, gender is often detrimental to success. "Pointing towards the Wild West brand of masculinity portrayed in hacker culture, the misogyny displayed by men who can hide behind the anonymity of the Internet and the association of technology with desire, eroticism, and artificial creation."[34] In addition to a criticism of hacker culture is that based on gender, hacker culture lacks a unified goal. However, hacktivism often has a political goal.

Feminist ethics provides a structure through which to critique the problem of women and non-binary people's oppression in hacker culture and the military. "A feminist approach to ethics asks questions about power—that is, about domination and subordination—even before it asks questions about good and evil, care and justice, or mothers and fathers."[35] The relevant analysis can be framed by three points. "Similarly, people who adopt a feminist approach to ethics are usually committed to the three normative goals that philosopher Alison Jaggar has identified. As she sees it, to count as a feminist approach to ethics, the approach must seek: 1) To articulate moral critiques of actions and practices that perpetuate women's subordination 2) To prescribe morally justifiable ways of revisiting such actions and practices 3) To envision morally desirable alternatives that will promote women's emancipation."[36] In an ideal system, the standard would be egalitarian for human beings. "It is to say that feminists pay attention to issues of power because in so doing they liberate themselves and others."[37]

Jaggar's analysis can be applied in the Ukraine IT Army example. First, an institution that perpetuates women's subordination is hacker culture.[38] Second, we can see that few women and non-binary people become hackers.[39] Third, Russia's invasion of Ukraine has resulted in an IT Army which is a combination of the military, hackers, and activism. The combination of the military, hackers, and activism is likely to promote gender emancipation because it is merit based, anonymous, and grounded in political ideology.

The notion that hacker communities are equal opportunity communities is not supported, but we might see that the Ukraine IT Army moves more towards a meritocracy where gender is a more minor factor. Women hackers are motivated by political activism and political activism has been spurred by Russia's invasion of Ukraine. Therefore, the number of women and non-binary hacktivists is likely to increase as a result of Russia's war on Ukraine.

ABOUT THE AUTHOR

Ellen Cornelius received her J.D. from the University of Maryland in 2005 and is a member of the Maryland Bar. Since joining CHHS in 2008, Ms. Cornelius has worked for the District of Columbia's Homeland Security and Emergency Management Agency, Maryland's Department of Health and Mental Hygiene, and Montgomery County Office of Emergency Management and Homeland Security. Ms. Cornelius teaches three courses at the University of Maryland Francis King Carey School of Law: Law and Policy of Cybersecurity, Legal Ethics, and Legal Analysis and Writing.

[1] I would like to thank Quinn Conlan (née Julianna Conlan, J.D. expected 2024, University of Maryland Carey School of Law) for her assistance with research for this article.
[2] https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
[3] https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
[4] Feminist Ethics (Stanford Encyclopedia of Philosophy)
[5] https://www.wilsoncenter.org/blog-post/ukrainian-women-make-strides-toward-political-engagement-barriers-remain
[6] https://www.wilsoncenter.org/blog-post/ukrainian-women-make-strides-toward-political-engagement-barriers-remain
[7] https://www.washingtonpost.com/politics/2021/10/11/hacktivists-are-back/
[8] https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html?referringSource=articleShare
[9] https://www.cnn.com/2022/02/24/europe/ukraine-russia-attack-timeline-intl/index.html
[10] Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says – The New York Times (nytimes.com)
[11] https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
[12] https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/
[13] Id.
[14] Id.
[15] Id.
[16] Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory | WIRED
[17] https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX
[18] Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory | WIRED
[19] https://www.reuters.com/technology/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-2022-03-01/
[20] Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory | WIRED
[21] https://www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia
[22] Id.
[23] Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory | WIRED
[24] https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
[25] Ukraine's "IT Army" of Hackers Take the Fight to Russia (foreignpolicy.com)
[26] Ukraine's "IT Army" of Hackers Take the Fight to Russia (foreignpolicy.com)
[27] https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
[28] Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says – The New York Times (nytimes.com)
[29] Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says – The New York Times (nytimes.com)
[30] Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says – The New York Times (nytimes.com)
[31] https://www.nbcnews.com/tech/security/study-reveals-age-nationality-motivation-hackers-n647171
[32] Part II: Female Hackers Face Challenges – ABC News (go.com)
[33] Part II: Female Hackers Face Challenges – ABC News (go.com)
[34] A.E. Adam, Hacking into Hacking: Gender and the Hacking Phenomenon. ACM SIGCAS Computers and Society, Volume 32, Number 7 (2004).
[35] Rosemarie Tong. Feminine and Feminist Ethics. Wadsworth Publishing Company, p. 160, 1993.
[36] Rosemarie Tong. Feminine and Feminist Ethics. Wadsworth Publishing Company, p. 10-11, 1993.
[37] Rosemarie Tong. Feminine and Feminist Ethics. Wadsworth Publishing Company, p. 183, 1993.
[38] Part II: Female Hackers Face Challenges – ABC News (go.com)
[39] https://www.nbcnews.com/tech/security/study-reveals-age-nationality-motivation-hackers-n647171