The Evolution of the IT Army of Ukraine

By Stefan Soesanto

Back in September 2020, Harvard's Belfer Center published the National Cyber Power Index, which utilized 32 intent and 27 capacity indicators to rank 30 countries according to their 'cyber power.' Ukraine was ranked 26th out of 30, while Russia scored fourth overall respectively.[1] In June 2021, the International Institute for Security Studies (IISS) released their "cyber power assessment" of 15 countries, with Ukraine not even making the cut.[2] Fast forward to September 2022 – roughly seven months into the Russian invasion – and Belfer now ranks Ukraine 12th out of 30, while Russia overtook the UK and is deemed the third strongest cyber power in the world, behind the US and China.[3] Two questions naturally open up: How did Ukraine jump 14 ranks within just two years? And why is the third most powerful cyber nation unable to dominate Ukraine in cyberspace?

The answer to both questions is that calculating 'cyber power' is an inherently difficult, complex, and maybe even futile task. As of this writing, we still do not fully understand the vast digital global ecosystem that has been 'militarized' and mobilized in the defense of Ukraine. We also do not yet exactly comprehend the role of Ukrainian digital ingenuity and talent, the significance of external technical and intelligence support, and grasp the underlying reasons for Russian failures in and through cyberspace. Similarly, the existence of the IT Army of Ukraine and its ability to successfully mobilize thousands of volunteers from across the globe to run Distributed Denial of Service (DDoS) attacks and more sophisticated operations against Russia's digital infrastructure, defies the very assumptions of centralization and state sovereignty that underpin the term 'power' – let alone 'cyber power.'

The conduct of the IT Army is still a very niche cyber topic for analysts, scholars, and lawmakers alike. As such, the IT Army of Ukraine will probably never make it onto the cover of the New York Times, even though it is exposes major deficiencies in how Western governments have been thinking about sovereignty in cyberspace, the principle of due diligence, attribution, non-government actors, and numerous other legal and policy issues. The barely existing public discussion on the IT Army, does not discount the relevance, effectiveness, and discernable impact the IT Army is already having on national cyber defense policies, the conduct of modern warfare, and international law applicable to cyberspace. By all accounts, The IT Army is Ukraine's most effective and proven tool to wage economic and information warfare in and through cyberspace against the Russian Federation. In its current form, it is neither civilian nor military, neither public nor private, neither local nor international, and neither lawful nor unlawful. The IT Army is a unique phenomenon the world has never seen before.

Back in June 2022, CSS published the – so far – only comprehensive study on the IT Army.[4] This chapter recaps some of study's past findings and provides a glimpse into the IT Army's evolutionary path forward. As with the CSS study, this chapter does not question Ukraine's right to self-defense, its existential struggle for survival, nor the fundamental need of the Ukrainian people to do everything in their power to stem the tide of the Russian invasion. Instead, the central question the study focused on is whether the IT Army's conduct is reconcilable with long held Western views on norms, international law, military targeting rules (i.e., distinction, military necessity, and proportionality), state sovereignty, civilian participation in an ongoing international armed conflict, fighting cybercrime etc. As of this writing, NATO and EU member states have refrained – for political reasons or otherwise – from providing answers to the fundamental legal and policy challenges the IT Army poses.

What is the IT Army of Ukraine?

The idea of creating the IT Army of Ukraine emerged sometime between February 24, when the Russia invasion began, and February 26. During that time frame, Yegor Aushev – a well-known Ukrainian IT entrepreneur and co-founder of Cyber Unit Tech, Cyberschool, and Hacken.io – met with Ukraine's Minister of Digital Transformation Mikhailo Federov to discuss the possibility of putting together an army of volunteers that would help defend and secure Ukraine's digital infrastructure. The discussion however did not result in a concerted effort by Aushev and Federov. Instead, they went their separate ways. Aushev and Cyber Unit Tech, in cooperation with the Ukrainian Ministry of Defense, assembled around 1000-1500 Ukrainian IT specialists to deploy across Ukraine's critical infrastructure companies. [5] Meanwhile, Federov realized that achieving dominance in the information warfare space (i.e., winning the propaganda war) was a preeminent necessity to significantly increase public support for the Ukrainian government on the domestic and international stage. With that in mind, Federov and his Ministry of Digital Transformation stood up the IT Army of Ukraine on February 26, by announcing on social media the creation of a Telegram channel called itarmyofukraine2022. Anyone around the world that was interested in participating in the IT Army would find all the relevant information in that channel. The first task of the IT Army: "use any vector of cyber and [Distributed Denial of Service] attacks on "31 Russian banks, businesses, and government websites."[6] Within Ukraine, the call to arms was even picked up by the Ukrainian Ministry of Education and Science, which invited "applicants for higher education, pedagogical, scientific, scientific and pedagogical workers of higher education institutions and the scientific community of Ukraine, [...] to join the work of the IT Army of Ukraine."[7]

DDoS attacks essentially overwhelm a website with requests and traffic to the extent that they slow down, become unreachable, and eventually collapses under the data load. In the United States, participating in DDoS campaigns and DDoS for hire services, is punishable under the Computer Fraud and Abuse Act and may result in arrest and criminal prosecution, leading to penalty or a significant prison sentence.[8]

When it comes to DDoS effectiveness, the IT Army is a lot more persistent that any other hacktivist and cybercriminal group before it. The IT Army can systematically keep websites down for days, weeks, and sometimes months on end, while hacktivists and cybercriminals tend to do so for only a few hours, on and off over a week or two. Thus, when we look at Russian online sales and services, the IT Army is able to impose significant economic costs to Russian businesses and create long-lasting customer dissatisfaction effects. On March 26, 2022, the itarmyofukraine2022 Telegram channel counted 307.165 subscribers.[9]

The activities of the IT Army do not function in isolation. There is an entire eco-system that has latched onto its activities, including numerous other DDoS groups, DDoS tool developers, hacktivists, data leak hosting platforms, and volunteers whose members are located both in and outside of Ukraine. Among them you will find Disbalancer's Liberator – a DDoS tool developed and financed by Estonian headquartered cybersecurity company Hacken.io – that is openly cooperating with the Ukrainian Ministry of Digital Transformation.[10] An offensive bug bounty program set up by Hackenproof – Hacken.io's bug bounty platform – which funnels vulnerabilities found in Russian critical infrastructure to the Ukrainian military and intelligence service. And a website with DDoS tools and instructions previously hosted at ddosukraine[.]com[.]ua, which the IT Army adopted, refined, and turned into their official website in April - now reachable at itarmy[.]com[.]ua. The IT Army's website provides instructions and links to various DDoS tools that were specifically developed for the IT Army, including MHDDoS_proxy, Db1000n, Distress, and uaShield. All of these DDoS tools are hosted on GitHub, the largest code hosting platform for version control and collaboration in the world. GitHub is owned by Microsoft. Curiously, in January 2023 GitHub disabled the accounts of pro-Russian hacktivist group NoName057(16) within a week, after researchers at Sentinel Labs reported the accounts for hosting DDoS tools that were used to hit entities in NATO countries, including Denmark's central bank.[11] GitHub explained its move by noting that "we disabled the accounts in accordance with GitHub's Acceptable Use Policies, which prohibit posting content that directly supports unlawful active attacks."[12] As of this writing, all of the IT Army's code repositories mentioned above, remain freely available on GitHub since the start of the invasion.[13]

The IT Army also maintains an in-house team – highly likely consisting of Ukrainian intelligence and military cyber operatives. Initially this team defaced Russian websites to spread disinformation and sow mistrust.[14] Then they began to pivot to more advanced operations, including their first offensive campaign that breached RuTube – a popular Russian Youtube clone – and almost succeeded in taking out the platform's infrastructure and deleting all its content.[15] Other campaigns include the sabotage of the Russian start-up Rossgram – a Russian Instagram clone, and dumping source codes and the internal data of Russian FinTech company Right Line which is developing in the government's Digital Ruble project.[16]

In October 2022, the IT Army released a video in which they proclaimed that the in-house team successfully breached the network of the LOESK thermal power plant which feeds the electricity grids of St. Peterburg and the Leningrad oblast. According to the IT Army, they "gained access to the operator's workstation and played with the switches," which led to outages in the Leningrad region. The IT Army also exfiltrated a trove of LOESK's customer databases, passports scans, internal documents, and technical schematics, which they dumped into the public domain.[17] On October 12, LOESK published a press release in which they said that they faced a "massive cyberattack that attempted to hack into the company's network structure" and that "the attack was completely neutralized preventing out-of-schedule outages for consumers."[18] With no word did LOESK mention the IT Army nor the blackouts that occurred.

On November 4, 2022, the IT Army released its latest video to date, which covers their campaign against Gazprombank back in September. The video shows how Alexander Egorkin, First Vice President of Gazprombank, spoke about the IT Army's campaign at the BIS Summit in Russia. According to Egorkin and the IT Army, Gazprombank was specifically targeted because it "is the only bank that conducts all payments for gas."[19] Meaning, it "is the bank through which all major government payments pass, including gas fees."[20] Egorkin further elaborated that the attack was "well done. First, they targeted the website. Second, the SMS providers. And third, the call center. [...] The attacks were great, done with creativity. [...] The attackers knew the entire pool of the banks IP addresses. Without exception. They even knew those who were not involved in the banking services."[21] Egorkin's praise of the IT Army is the first public admission of the group's effectiveness by a major Russian company. It also provides a glimpse into the ongoing digital onslaught taking place in Russia's digital space.

What makes the IT Army problematic?

The IT Army was stood up by the Ukrainian Ministry of Digital Transformation to assemble, train, and direct people from across the globe (including NATO and EU citizens), to participate in persistent DDoS campaigns against Russian civilian infrastructure amidst the ongoing international armed conflict in Ukraine.

As of this writing, neither NATO nor EU member states have figured out what the exact legal status of those citizens is, who are participating in the IT Army's activities while being physically located on NATO/EU territory. Back in early March 2022, Victor Zhora – chief digital transformation officer at Ukraine's State Service of Special Communication and Information Protection (SSSCIP) – explained that "homegrown volunteers were attacking only what they deem military targets, in which he included the financial sector, Kremlin-controlled media and railways."[22] But over the course of war, the IT Army's targeting selection naturally expanded to achieve specific effects and harness distinct opportunities. As a result, Russian universities were targeted to obstruct student enrollment processes, and the websites of online pharmacies, electronic stores, car dealerships, food delivery services, movie theaters, and freelance platforms were taken out to disrupt Russia's society and economy at large.[23] The overall dictum the IT Army seems to follow is that any domain and service ending in .ru is a potential legitimate target.

At Microsoft's European Cyber Agora in June 2022, the issue of the IT Army came up during the closed workshop session titled 'War in Ukraine: Lessons for the EU's cyber diplomacy.' On this very rare occasion, one senior official from the European External Action Service (EEAS) admitted that they had no idea how to categorize nor handle EU citizens that participate in the activities of the IT Army. As such, the official simply quipped that "they are cyber criminals that need to be prosecuted. How do we do that?"[24] None of the workshop participants had an answer. But even if they came up with one, their solution would probably not have accounted for several crucial details.

The IT Army's targeting process significantly evolved over the course of the war. Nowadays, it is much more refined, intelligent, and nimble than anything we seen practiced in the past by hacktivists and cybercriminal groups alike. The evolutionary change in the IT Army's targeting selection process highly likely coincides with the managerial takeover of the IT Army by the Ukrainian intelligence service (SBU) and the Ministry of Defense. Back in June, our CSS study already noted that "it is highly questionable whether the Ministry of Digital Transformation has the legal authority to independently setup the IT Army [...] without any coordination or control exercised by Ukraine's defense and intelligence services."[25] For around three months after our study was published, this assessment was questioned (and sometimes attacked) by analysts, pundits, and even by those actively participating in the IT Army's DDoS activities themselves.

In late-September the narrative was finally settled. Huib Modderkolk, an investigate reporter working for the Dutch newspaper De Volkskrant, received a tip that a Dutch Special Forces veteran - going by the online handle 'Hactic' - was part of the inner circle of the IT Army. After months of back and forth, Huib eventually succeeded in meeting and interviewing Hactic in his home somewhere in the Netherlands. Huib's article, published on September 24 and titled 'Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol' (Engl. translation: An international cyber army against Russia with a Dutchman in the leading role), provides the first-ever personal account of the IT Army's internal workings. Among other items, Hactic explained that "about 25 to 30 'generals' form the management [of the IT Army], they consist of employees of the Ukrainian secret service and Ukrainian government. The 'colonels' [of whom Hactic is one] are below, these administrators, hackers and malware specialists are 'manually' selected by the generals and participate in offensive actions [i.e., the IT Army's in-house team]."[26]

Hactic also explained that he wrote a document outlining what the rules and behavioral norms for the IT Army were supposed to be. In it, he prescribed that schools, pharmacies, orphanages, hospitals, and nuclear installations were off limits, because the IT Army did not want to cause physical harm to Russian civilians. During the interview, Hactic further elaborated that "few volunteers realize that if you actively participate in the cyber war, you are automatically considered a combatant in that war." While, as of this writing, legal scholars and Western governments have avoided to publicly opine about the legal status of these volunteers and the lawfulness of the IT Army's DDoS activities, it was refreshing to hear that Hactic and the IT Army's managerial team were indeed aware of the potential dangers. That being said, the thousands of people from across the globe that participate in the IT Army's DDoS activities, should not be viewed as cybercriminals as the EEAS proposed. In fact, they are replaceable and discardable pawns used by Kyiv in the ongoing Ukrainian intelligence and military cyber operation that is the IT Army. For EU and NATO governments, the IT Army's reliance on EU/NATO citizens to run their operations, poses significant legal and policy questions within the individual member states. For political reasons or otherwise, these questions remained unaddressed.

Similarly, the volunteers that actively contact the IT Army to offer their skillsets and get accepted – as Hactic was –, are likely people with previous intelligence or military experience. The 2019 investigation by Reuter's Christopher Bing and Joel Schectman into Project Raven has vividly shown how former NSA operatives were handsomely paid to use their skills to help the United Arab Emirates spy on dissidents, political rivals, journalists, and human rights activists.[27] Given that strongly held ideological believes, in combination with a need to right wrongs and resist injustices, are an even more powerful motivator for people to join a cause than financial compensation is, we can probably confidently assume that Hactic is far from the only foreign veteran that has joined or offered his skills to the IT Army. A second indicator, is the size of the Ukrainian Foreign Legion, which supposedly numbers around 20.000 non-Ukrainians that have volunteered to fight and die for Ukraine on the kinetic battlefield.[28] If 20.000 foreigners are willing to travel to Ukraine to participate in the fighting, then how many foreigners have likely offered their hacking skills to join the IT Army from the safety and comfort of their own homes thousands of miles away from Ukraine? The final indicator is that starting in December 2022, the IT Army has been searching for a 'Secretary of Education.'[29] According to the IT Army's website, the tasks would entail: processing volunteer applications received through their online form, provide candidates with test tasks prepared by the [in-house] specialists, and serving as a mediator between the specialists and the candidate during the application decision-making process.[30] It is unknown how many volunteer applications the IT Army receives per a month, but it must be quite a significant amount if they are hiring a separate person to manage it.

Another issue that makes the IT Army problematic is that people are urged to use virtual private networks (VPNs) for their DDoS attacks. VPNs normally serve the purpose of establishing a secure connection to another network or device (think logging into your company's internal network from your computer at home). However, in the context of the IT Army, the usage of VPNs is due to its ability to also cloak your public IP behind a server in another country. Meaning, the DDoS attack is run by a DDoS tool on a computer in country A, travels through the VPN connection to a server located in country B, and then server B sends the DDoS traffic to the target in Russia. Thus, from a target's perspective, the DDoS attack might be coming from a server in Finland, when it is actually being generated by a computer sitting in France. Similarly, the IT Army has been instructing people to install DDoS tools on virtual machines (VMs) which are hosted on cloud service providers (think Google Cloud, Amazon Web Service, DigitalOcean, or Hetzner). With that method, a person does not even have to turn on his own computer, because the virtual machine on the cloud server will run the DDoS attack 24/7/365 or until the cloud provider bans the customer's account. In sum, the private sector's VPN and cloud server infrastructure – which is predominately located on NATO and EU territory due to strong privacy and data protection regulations – is being used by people across the globe to funnel through and run the IT Army's DDoS campaigns. This setup is naturally unaffected by the electricity outages and power supply problem that are plaguing Ukraine due to Russian bombardments. To the surprise of no one, on June 10, 2022, the Russian Foreign Ministry declared that "according to experts, in order to carry out massive DDoS attacks involving 'cyber volunteers', attackers use malicious software based on the servers of Hetzner (Germany) and DigitalOcean (USA) supplier companies. Foreign specialized platforms (War.Apexi.Tech, Ban-Dera.com) are actively used, the online capacities of IPstress.in and Google servers are regularly used."[31]

On top of this, there are two additional problem sets. First, for a while, the IT Army officially partnered up with IPStress[.]in – their only partner at that time - showing the company's logo prominently on the bottom of their website. The problem is that IPStress[.]in is an IP boot stresser that maintains its own botnet to DDoS websites. In essence, a cybercriminal enterprise. On May 31, 2022, the FBI and the US Department of Justice (DoJ) seized the ipstress[.]in domain and others. In its press release the DoJ explained that IPStress "publicly offered to conduct 'Distributed Denial of Service' attacks, or 'DDoS' attacks for clients – specifically, a format called booter or stressor attacks. [...] The seizures of these domains were part of a coordinated law enforcement action with the National Police Corps of the Netherlands and the Federal Police of Belgium. The actions executed by our international partners included the arrest of a main subject, searches of several locations, and seizures of the webserver's infrastructure."[32] In sum, the IT Army – a construct that was stood up by the Ukrainian Ministry of Digital Transformation and is managed by the Ukrainian intelligence service, officially partnered up with a cybercriminal enterprise outside of Ukraine in their quest to more efficiently DDoS Russia's digital infrastructure.

The second problem is that most of the cloud service providers that the IT Army is misusing – so far without any repercussions – for its DDoS attacks, are also hosting Ukrainian government data. Amazon's AWS for example was the first organization that helped move Ukrainian government data into their cloud environment when Russian tanks were amassing at the Ukrainian border.[33] According to Federov, "Amazon AWS literally saved our digital infrastructure – state registries and critical databases migrated to AWS cloud environment."[34] Microsoft equally stepped up during the same time frame by moving "16 of the 17 Ukrainian ministries' data to the cloud" onto servers outside Ukraine.[35] In November 2022, Microsoft committed itself to provide "additional technology aid valued at roughly $100 million, which will ensure that government agencies, critical infrastructure and other sectors in Ukraine can continue to run their digital infrastructure and serve citizens through the Microsoft Cloud."[36] Google also offered its services for free by – among other items - expanding the eligibility for Project Shield, which provides free, unlimited protection against Distributed Denial of Service (DDoS) attacks." The service is available to certain public sector organizations, which "includes Ukrainian government websites and embassies worldwide."[37] As of this writing it is unclear whether and how Amazon, Microsoft, and Google are balancing the risks between helping the Ukrainian government survive on the one hand, and its own services and infrastructure being misused by the IT Army on the other. Federov, who literally stood up the IT Army, awarded all three companies the Ukrainian Peace Price on the sidelines of the Ukraine Recovery Conference in Lugano, Switzerland, on July 4-5, 2022.[38]

Where is the IT Army evolving toward?

The IT Army is a well-managed organization that is flexible enough to seamlessly evolve and adapt to new challenges. In the early days of the invasion, the IT Army simply designated

DDoS targets by posting merely the URLs of a target in their Telegram channel, ex. ria[.]ru and sberbank[.]ru. During that timeframe, the IT Army did not yet have a website, nor any shareable document that would instruct people where to download and how to use DDoS tools. Everything was very amateurish and planless, so people started to help each other out by communicating in the IT Army's Telegram chat. The problem with that approach was that anyone could post anything in the chat, including redirecting people to phishing sites and malicious downloads. The IT Army could have died there, but it didn't.

Gradually, the IT Army refined its conduct. In addition to the URLs, they started to post IPs and port numbers to target specific servers and services. They also reduced the number of daily targets to focus their traffic DDoS attacks, rather than spreading it out across multiple targets. Around late-March the IT Army also began to target multiple subdomains of one single company. On March 26 for example, they DDoS'd 19 different subdomains of cse[.]ru, one of Russia's largest courier parcel delivery service.[39] The IT Army also began to share a Google docs document (i.e., the 'IT Army Coordination Document') in their Telegram chat, which provided people with basic instructions on what DDoS tools to download, where to find them online, and how to run them. Starting in April 2022, the website ddosukraine[.]com[.]ua was eventually incorporate as the official IT Army website by moving it to the itarmy[.]com[.]ua domain. The Coordination Document subsequently seized to exist.

The IT Army has also been attempting to counter-act and find workable solutions to stem the continuous decrease in user participation. At its height in March, the IT Army's Telegram channel counted 307.165 subscribers. As of this writing, it has 202.668. That is a 34 per cent decrease over 11 months. On average, the IT Army is losing 100 subscribers per day. While it is still unknown why exactly they are losing this many followers so quickly, the likeliest explanation is a combination of (a) the IT Army not being seen as novel anymore, (b) simple boredom due to repetitive tasking, and (c) the ongoing kinetic war itself, which remains largely unaffected by the IT Army's DDoS activities.

The solutions the IT Army has come up with are manyfold. On the one hand, they have set up a Telegram bot to automate the timing of the DDoS attacks. The way it works is that people essentially make instances on their cloud servers available to the IT Army channel administrators by creating a .csv file (which includes the server name, username, password, IP, and port) and send it to the Telegram bot. With that access, the IT Army administrators can direct all accessible cloud servers against a specific target. As the IT Army website explains it: "Anyone can make their cloud servers available for use (which they started manually) and + create as many free servers as they want and also transfer them to use with the help of a bot. It turns out that depending on the number of users and the number of servers provided, the strength of the attack will depend, but the coolest thing is that the attack will be launched by admins asynchronously, that is, you will no longer have to do it yourself."[40]

On October 1, 2022, the IT Army additionally introduced a way for people to track their own personal DDoS statistics.[41] To do so, they the developers behind MHDDoS_proxy, Db1000n, and Distress implemented a user-id parameter to easily pull individual DDoS statistics from all three tools. All a user must do, is get a unique user-id assigned by the IT Army's Telegram stat_bot.[42] Other pro-Ukraine DDoS groups have implemented similar features. For example, Hacken's Disbalancer hands out samurai ranks to users in their Telegram channel, based on their activity using their DDoS tool Liberator.[43] On February 10, the IT Army announced the creation of a leaderboard on its website that tracks the "top-15 mhddos_proxy users based on [the] generated traffic during the week."[44]

All these developments, point into one particular evolutionary direction. On the DDoS side, the IT Army will continue its push toward automatization and gamification to stem the loss of volunteers. On the in-house side, we are likely witnessing a growing influx of specialized volunteers, and as a result a future increase in the number of breaches, data dumps, and wiper campaigns conducted by the in-house team. Overall, the IT Army of Ukraine will highly likely become the first Ukrainian advanced persistent threat (APT) actor – or the second Ukrainian APT behind Cloud Atlas.[45]

The term APT was coined by Greg Rattray back in 2007.[46] Nowadays it is used to describe a state actor that "uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences."[47]

Is the IT Army a model for others to emulate?

Governments around the world will highly likely adapt, emulate, and learn from the multitudes of ad-hoc projects that are currently enabling the Ukrainian government to resist and fight back against Russia in and through cyberspace. Understanding the IT Army is a central piece to this overarching learning process and finding distinct answers to the larger question of how to practically wage warfare in and through cyberspace in the absence of absolute dominance.

That being said, Western militaries will highly likely be unable to officially stand-up their own versions of the IT Army, due to numerous domestic legal hurdles and the growing awareness that the IT Army of Ukraine's organizational setup highly likely violates international law (think state sovereignty) and undermines established norms regarding state behavior in cyberspace. Instead, what will likely occur is that intelligence services across the globe will take the lead in outlining, pre-planning, and testing a variety of IT Army-like structures, narratives, and trigger events that will mobilize volunteers around the globe into action when needed. This 'activation' of volunteers will highly likely also come into play during peace time outside an international armed conflict. Meaning, social causes and non-governmental organizations might potentially be used as cover identities or might be indirectly enabled to replicate ad-hoc IT Army-like structures to run their own campaigns in and through cyberspace. Another worrying potential evolution could be a shift away from DDoS toward the popularization of other attack vectors. Imagine for example if an intelligence service would publicly post detailed manuals, readily available tools, and a continuously updated target list for volunteers across to run their own individual ransomware campaigns. What would this do to process of attribution? The aim of combatting cybercrime? And the idea of militaries adhering to the law of armed conflict?

Taiwan's intelligence community might be the likeliest entity to successfully replicate the current IT Army's setup in reaction to an imminent or ongoing Chinese invasion of the island. As with the IT Army of Ukraine, an IT Army of Taiwan would highly likely continue its activities even after the capital has fallen and the entire country were to be occupied. An IT Army consisting of volunteers from around the globe, and led by an intelligence service, is probably the one entity that will continue to fight and evolve no matter the developments on the kinetic battlefield. As of this writing, there are no indications that the IT Army will be dissolved anytime soon.

[1] The NPCI 2020 looked at 30 countries but only listed 29 (excluded the DPRK due to insufficient information). See: Julia Voo et al., "National Cyber Power Index 2020," *Harvard Belfare Center*, September 2020, 11.

[2] IISS, "Cyber Capabilities and National Power – A Net Assessment," *International Institute for Strategic Studies*, 28.06.2021.

[3] Julia Voo et al. "National Cyber Power Index 2022," *Harvard Belfare Center*, September 2022, 10.

[4] Stefan Soesanto, “The IT Army of Ukraine – Structure, Tasking, and Ecosystem,” *Center for Security Studies/ETH*, June 2022.
[5] CyberUnit.Tech, “How Ukrainian Cyber Army was created,” medium.com, 05.07.2022
[6] IT Army of Ukraine, “Завдання #1 Закликаємо вас використовувати будь-які вектори кібер та DDoS атак на ці ресурси,” Telegram, 26.02.2022.
[7] Ministry of Education and Science of Ukraine, “МОН ЗАПРОШУЄ ДОЛУЧИТИСЯ ДО РОБОТИ IT-АРМІЇ УКРАЇНИ,” *mon.gov.ua*, 05.03.2022; Ministry of Education of Science of Ukraine, “Керівникам закладів вищої освіти та наукових установ України,” *mon.gov.ua*, 04.03.2022.
[8] FBI, “The FBI and International Law Enforcement Partners Intensify Efforts to Combat Illegal DDoS Attacks,” fbi.gov, n.d.
[9] Tgstat, “IT Army of Ukraine – Subscribers number growth,” *tgstat.com*, n.d.
[10] Yegor Aushev sold his stake in Hacken.io in late-2019. In March 2022, Politico reported that some 50 employees of Hacken’s Kyiv office (which the Disbalancer team is part of) relocated to Spain. On May 12, the Wall Street Journal covered Hacken as well and noted that Kyiv’s Hacken team moved on to Lisbon, Portugal. See: Laurens Cerulus, “Kyiv’s hackers seize their wartime moment,” *Politico.eu*, 10.03.2022; David Uberti, “They Fled Ukraine to Keep Their Cyber Startup Alive. Now, They’re Hacking Back,” *The Wall Street Journal*, 12.05.2022.
[11] AJ Vincens, “GitHub disables pro-Russian hacktivist DDoS pages,” *Cyberscoop*, 12.01.2023.
[12] Ibid.
[13] IT Army of Ukraine, “Instructions to configure DDoS Attacks to Enemy Country,” itarmy.com.ua, n.d.; Porthole-ascend-cinnamon, “mhddos_proxy,” Github, n.d.; Arriven, “db1000n,” Github, n.d.; Yneth, “Distress-releases,” Github, n.d.; Opengs, “uashield,” Github, n.d.
[14] IT Army of Ukraine, “Miller is against the war, and Sukhoi lacks of details for aircraft — IT-army spreads the truth,” Youtube, 23.04.2022.
[15] IT Army of Ukraine, “Взлом Rutube: самая большая победа кибервойны!” Youtube, 14.05.2022.
[16] IT Army of Ukraine, “Нове звернення IT-армії. Російський Росграм, іди на х#й,” Telegram, 07.04.2022; IT Army of Ukraine, “Большая утечка данных о финансовых операциях в россии и беларуси. Рассказывает IT-армия Украины,” Youtube, 09.09.2022.
[17] Sudo rm -RF, “Destruction of the ua infrastructure = destruction of ru IT infrastructure,” Twitter, 11.10.2022.
[18] Loesk, “Специалисты АО «ЛОЭСК» отразили кибератаку на сетевую инфраструктуру компании,” *loesk.ru*, 12.10.2022.
[19] IT Army of Ukraine, “Газпром заценил атаку на себя. Привет от IT-армии Украины,” Youtube, 04.11.2022.
[20] Ibid.
[21] Ibid.
[22] Frank Bajak, “Ukraine digital army brews cyberattacks, intel and infowar,” *AP News*, 03.05.2022.
[23] Lukas Mäder, “Im Ukraine-Krieg kämpft eine «IT-Armee» online gegen Russland. Die Freiwilligen attackieren sogar Apotheken und Universitäten,” *NZZ*, 23.06.2022; Stefan Soesanto, “The IT Army of Ukraine – Structure, Tasking, Ecosystem,” *Center for Security Studies/ETH*, June 2022; IT Army of Ukraine, “Сьогодні продовжуємо нещодавну автомобільну тему,” Telegram, 16.09.2022; IT Army of Ukraine, “Віддалена робота на російських біржах фріланса,” Telegram, 12.12.2022; IT Army of Ukraine, “Ви добре попрацювали! Додаємо нові фріланс біржі,” Telegram, 26.12.2022.
[24] European Cyber Agora, June 15, 2022, Workshop 3: War in Ukraine: Lessons for the EU’s Cyber diplomacy.
[25] Stefan Soesanto, “The IT Army of Ukraine – Structure, Tasking, Ecosystem,” *Center for Security Studies/ETH*, June 2022, 23.
[26] Huib Modderkolk, “Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol,” *De Volkskrant*, 24.09.2022.
[27] Christopher Bing / Joel Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries,” *Reuters*, 30.01.2019.
[28] Andy Blatchford, “Band of others: Ukraine’s legions of foreign soldiers are on the frontline,” *Politico.com*, 24.03.2022.
[29] IT Army of Ukraine, “волонтерство,” itarmy.com.ua, n.d.
[30] IT Army of Ukraine, “волонтерство,” itarmy.com.ua, n.d.
[31] Russian Ministry of Foreign Affairs, “Ответ специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В.Крутских на вопрос СМИ об атаках на объекты российской критической инфраструктуры,” *mid.ru*, 09.06.2022.

[32] US Department of Justice, "WeLeakInfo.to and Related Domain Names Seized," *justice.gov*, 31.05.2022.
[33] Amazon Staff, "Safeguarding Ukraine's data to preserve its present and build its future," *aboutamazon.com*, 09.06.2022.
[34] Mykhailo Federov, "One more Peace Prize by @ZelenskyyUa comes to @awscloud," Twitter, 06.07.2022.
[35] Kevin Poireault, "Interview: Microsoft Shares Its Experience of Migrating Data in Times of Cyber Warfare," *infosecurity-magazine.com*, 30.09.2022.
[36] Brad Smith, "Extending our vital technology support for Ukraine," *blogs.microsoft.com*, 03.11.2022.
[37] Phil Venables, "Google Cloud's security and resiliency measures for customers and partners," *cloud.google.com*, 03.03.2022.
[38] Simon Sharwood, "Microsoft, AWS awarded Ukraine peace prize for cloudy services," *The Register*, 07.07.2022.
[39] IT Army of Ukraine, "Доброго ранку, IT армія!" Telegram, 26.03.2022.
[40] IT Army of Ukraine, "БОТ ДЛЯ ПОВНОЇ АВТОМАТИЗАЦІЯ DDOS АТАК НА РУСНЮ," itarmy.com.ua, n.d.
[41] IT Army of Ukraine, "Доки на росії примусово мобілізують нове гарматне м'ясо, ми посилюємо наш IT-фронт," Telegram, 01.10.2022
[42] IT Army of Ukraine, "статистика," itarmy.com.ua, n.d.
[43] Disbalancer, "The Most Active disBalancers Have Received Samurai Ranks," *blog.disbalancer.com*, n.d.
[44] IT Army of Ukraine, "Айтівці, наступного тижня ми запускаємо пілотну версію лідерборду," Telegram, 10.02.2023'; IT Army of Ukraine, "ТОП15 ЮЗЕРІВ MHDDOS ПО ТРАФІКУ ЗА ТИЖДЕНЬ," itarmy.com.ua, n.d.
[45] Note: Cloud Atlas might be the first Ukrainian APT. To date, no high confidence attribution assessment has been made as to its origin. See: Check Point, "Cloud Atlas targets entities in Russia and Belarus amid the ongoing War in Ukraine," *research.checkpoint.com*, 09.12.2022.
[46] Richard Bejtlich, "Greg Rattray Invented the Term Advanced Persistent Threat," *taosecurity.blogspot.com*, 10.10.2022.
[47] Kaspersky, "What Is an Advanced Persistent Threat (APT)?" *kaspersky.com*, n.d.