The Hague Centre
for Strategic Studies

Ukraine's Counter-Hybrid Campaigns in Cyberspace

Stefan Soesanto

November 2023

The Hague Centre
for Strategic Studies

Ukraine's Counter-Hybrid Campaigns in Cyberspace

Author:
Stefan Soesanto

November 2023

The report is a guest contribution, part of the HCSS Hybrid Threat paper series.

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Cover photos: Anton Holoborodko , https://commons.wikimedia.org/wiki/File:2014-03-09_-_Perevalne_military_base_-_0117.JPG, DVIDSHUB, Flickr - DVIDSHUB - Terrorism Training in New York.jpg - Wikimedia Commons, Mehr News Agency

Table of Contents

Summary

In reaction to the Russian invasion of Ukraine on February 24, 2022, the Ukrainian government stood up a variety of digital services and volunteer groups to counter Russia's aggression in and through cyberspace. This paper focuses on two Ukrainian hybrid warfare creations and their activities within the period from February 2022 to July 2023: The IT Army of Ukraine (IT-армія України) which are conducting DDoS and destructive cyber operations in and through the cyber domain, and the Internet Force of Ukraine (Інтернет Війська України) who are active on the information warfare front. The paper is part of a paper series on counter-hybrid warfare campaigning published by the The Hague Centre for Strategic Studies. It provides readers with insights into (a) how the IT Army and Internet Forces are internally organized and structured, (b) how they function and conduct their campaigns, (c) how they are incorporating volunteers from across the globe and at home, and (d) how these two groups are linked to the Ukrainian government. The paper also touches upon broader questions, such as (e) the discernible impact of these campaigns, (f) the subsequent complications for law of armed conflict, and (g) what lessons could be learned.

The IT Army of Ukraine

On February 26, 2022, Ukrainian Minister of Digital Transformation Mykhailo Federov announced the creation of the IT Army of Ukraine on Telegram, Facebook, and Twitter.[1] Conceptualized as an international volunteer force, anyone willing to participate was asked to join the IT Army's Telegram channel and tasked to "*neutralize the enemy's information propaganda*."[2] At its height, on March 27, 2022, the channel counted 307.186 subscribers from across the world.[3] As of this writing, the number stands at 172.810 subscribers, with an average loss rate of 4.461 subscribers per month.[4]

Throughout the course of the war, the IT Army naturally evolved to the extent that nowadays it can be separated into two distinct parts: (1) a Distributed Denial of Service (DDoS) component that supplies volunteers from across globe with the tools and knowledge to participate in the IT Army's centrally managed DDoS efforts. And (2) a professional in-house team, that selectively recruits highly skilled volunteers from across the globe to conduct more complex cyber operations, including destructive ones.

DDoS Targeting

In the early weeks of the invasion, the DDoS efforts of the IT Army were exclusively organized in the group's Telegram channel. The channel was primarily used to announce DDoS targets. Meaning, the channel moderators would post URLs, IPs, and ports of the websites that user were tasked to DDoS. Initially, the target selection process was aimed purely at the most well-known .ru domains, such as kremlin.ru or tass.ru. Over time though the process evolved to become more refined, sector focused, and more time sensitive. For example, during the university course enrollment period in Russia, the IT Army would DDoS Russian university websites. Similarly, at the end of the Russia tax filing season, the IT Army would disrupt local and federal tax service websites. The IT Army's self-declared mission is not to interfere in the kinetic war on the battlefield, but to "*help Ukraine win by crippling aggressor economies, blocking vital financial, infrastructural and government services, and tiring major taxpayers.* [...] *We want every resident of aggressor countries to feel and tire from their state's aggression*."[5]

1 Mykhailo Federov, "У нас дуже багато талановитих українців у цифровій сфері," Telegram, February 26, 2022, http://t.me/zedigital/1114; Mykhailo Federov, "У нас дуже багато талановитих українців у цифровій сфері," Facebook, February 26, 2022, https://www.facebook.com/mykhailofedorov.com.ua/posts/1005386320078887; Mykhailo Federov, "We are creating an IT army. We need digital talents," Twitter, February 26, 2022, https://twitter.com/FedorovMykhailo/status/1497642156076511233

2 Кабінет Міністрів України, "Мінцифри створило 3 сервіси, щоб боротися з окупантами на цифровому фронті," kmu.gov.ua, March 12, 2022, https://www.kmu.gov.ua/news/mincifri-stvorilo-3-servisi-shchob-borotisya-z-okupantami-na-cifrovomu-fronti

3 Tgstat, "IT Army of Ukraine – Subscribers number growth," n.d., https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers

4 Tgstat, "IT Army of Ukraine," n.d., https://web.archive.org/web/20230718090908/https://tgstat.com/channel/@itarmyofukraine2022/stat

5 IT Army, "Our Mission," itarmy.com.ua, n.d., https://itarmy.com.ua/?lang=en or https://archive.ph/68aJ7

The majority of targets are highly likely planned out weeks – if not months – in advance.

According to the IT Army itself, their targeting process goes through five steps: (1) analyze the targets by priority and assess their security; (2) on weekdays: target businesses and government institutions, on weekends target entertainment [including food delivery services, movie theaters, etc.]; (3) attack new or prior targets if vulnerabilities persist; (4) the best time to attack is when the target is in high demand; and (5) attack 24/7. Small effects are better than none.[6] It is unknown who exactly within the IT Army decides which sites will be DDoS'd. While a small fraction of targets is likely opportunistic, news cycle depended, or based on user recommendations – which can be submitted via the IT Army's website, the majority of targets are highly likely planned out weeks – if not months – in advance.

On February 20, 2023, the Ukrainian Ministry of Digital Transformation summarized that over the past year, "*the team attacked about 2240 targets, which is more than 15 thousand resources with unique IP addresses. These were hostile goals, from blocking the propaganda media of the occupiers to suspending the websites of Russian companies and banks.*"[7] Roughly five months later the Ministry added that, "*thanks to* [the IT Army's] *work, the volume of DDoS attacks on Russian Internet resources increased by 58% in 6 months of 2023, compared to 2022.*"[8]

DDoS Tools

Curiously, in the early days of the war, the IT Army did not link to or recommend any DDoS tools. Instead, it simply encouraged everyone to "*use any vectors of cyber and DDoS to attack."*[9] The IT Army could have died in its early days, because users began to download random tools and clicked on malicious links posted in the IT Army Telegram chat. To overcome this problem, the IT Army eventually disseminated a Google Docs document that recommended specific DDoS tools and provided rudimentary instruction guides. In April 2022, the IT Army eventually launched its own official website, which nowadays serves as the hub for DDoS tool sourcing and instructions.

As of this writing, the IT Army has endorsed four DDoS tools as its official ones: mhddos_proxy, db1000n, Distress, and UaShield.[10] All four are hosted on Microsoft-owned Github – the largest code-repository in the world. All four were developed by Ukrainian citizens and they closely cooperate with the IT Army to fulfill its needs. For example, in July 2022, the developers of mhddos_proxy noticed that their source code was increasingly being used by "*hostile*" parties. The IT Army therefore announced that "*the only solution, according to* [the] *developers, was to close the source code.* [...] [mhddos_proxy] *will now work exclusively for IT Army purposes. We still have access to the source code, so we can speak about its complete security and reliability.*"[11] Three of the four tools can also be installed via the official UkITA installer – a program the IT Army published to simplify DDoS installations. The UkITA installer also enables users to track their individually generated DDoS volume via a unique ID that can

6 https://t.me/itarmyofukraine2022/1207 or https://archive.ph/BFok0

7 Мінцифра, "Підсумки роботи IT-армії. Як українські IT-волонтери забезпечували кіберфронт," Telegram, February 20, 2023, https://t.me/mintsyfra/3834 or https://archive.ph/DjG6O

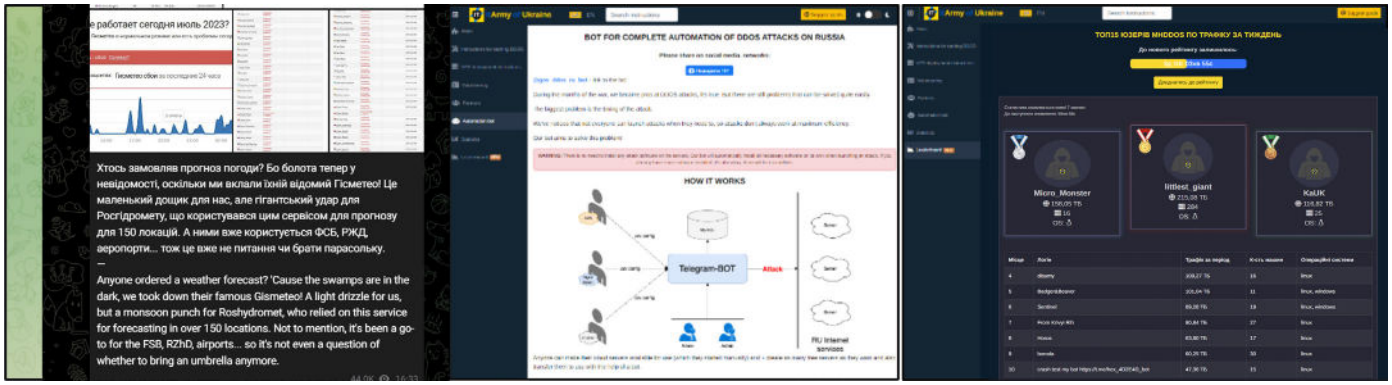
8 Мінцифра, "Викриті дані сотень тисяч росіян та постійні DDoS-атаки," Telegram, June 28, 2023, https://t.me/mintsyfra/4241 or https://archive.ph/AVD04

9 IT Army, "Завдання #1 Закликаємо вас використовувати будь-які вектори кібер та DDoS атак на ці ресурси," Telegram, February 26, 2022, https://t.me/s/itarmyofukraine2022/1 or https://archive.ph/SMt31

10 IT Army, "ІНСТРУКЦІЇ З НАЛАШТУВАННЯ DDOS АТАК НА КРАЇНУ ВОРОГА," itarmy.com.ua, n.d., https://itarmy.com.ua/instruction/ or https://archive.ph/Nbvi7

11 IT Army, "Вийшло чергове оновлення mhddos_proxy, що спрощує його використання та покращує безпеку," Telegram, July 12, 2022, https://t.me/itarmyofukraine2022/479 or https://archive.ph/jjMn4

be requested from the IT Army's Telegram bot.[12] The top 15 highest DDoS volume generating individuals are displayed every week on the IT Army's leaderboard.[13] The leaderboard was highly likely created to (a) combat the steady loss of user by gamifying DDoSing, and (b) to visibly acknowledge the contribution of the likely professional high rolling DDoSers.



Source: (left) IT Army Telegram post on July 20, 2023, covering their DDoS campaign against Gismeteo; (center) Cloud login-sharing and bot automatization explanation on the IT Army website; (right) User DDoS leadership board on the IT Army website.

DDoS Management

In early-October 2022, the IT Army fundamentally changed how it would interact with its users. The group realized that Russian companies and cybersecurity firms increasingly used the publicly posted targeting information to "*make quick fixes that undermined the* [IT Army's DDoS] *efforts*."[14] As a result, the IT Army stopped posting targeting information publicly, which also meant that its global volunteers force had far less visibility into which websites the IT Army's DDoS traffic was aimed at. Essentially, the IT Army's DDoS campaigns were now completely centrally directed as the DDoS tools automatically pulled their target list from one central source. As a communication replacement, the IT Army's Telegram channel started to post DDoS after-action reports to inform its user. Among other items, the posts included screenshots of Russian citizens complaining on social media about the unavailability of a target's web service.[15]

As of late, the IT Army has become very selective about its DDoS targeting and after-action reporting. For example, in the entire month of July 2023, the IT Army merely talked about five DDoS campaigns: They took out the website of the Russian traffic police,[16] Russian

12 IT Army, "БОТ ДЛЯ ОТРИМАННЯ ПЕРСОНАЛЬНОЇ СТАТИСТИКИ DDOS АТАКИ НА РУСНЮ," itarmy.com.ua, n.d., https://itarmy.com.ua/statistics/ or https://archive.ph/u9w2Y

13 IT Army, "ТОП15 ЮЗЕРІВ MHDDOS ПО ТРАФІКУ ЗА ТИЖДЕНЬ," itarmy.com.ua, n.d., https://itarmy.com.ua/leaderboard/ or https://archive.ph/L8Qiq

14 IT Army, "Раніше на сайті публікувався детальний перелік ресурсів," Telegram, October 2, 2022, https://t.me/itarmyofukraine2022/740 or https://archive.ph/w2Azr

15 IT Army, "Через нашу сьогоднішню атаку на Сбер ID у клієнтів Сбербанку збій з самого ранку," Telegram, October 7, 2022, https://t.me/itarmyofukraine2022/765 or https://archive.ph/ul20w

16 IT Army, "Сайт ГІБДД росії," Telegram, July 25, 2023, https://t.me/itarmyofukraine2022/1453 or https://archive.ph/HQCTX

railways,[17] the weather forecast service Gismeteo,[18] telecommunications provider Beenet,[19] and Luganet – an internet provider in the Luhansk Oblast.[20] It is unknown whether the IT Army targeted any other websites or services during that time period.

From a management perspective, the DDoS component of the IT Army is highly responsive, nimble, quasi-transparent, and well-integrated into its surrounding ecosystem. As such, it likely consists of at least five distinct teams: (1) a targeting and probing team, (2) a software engineering and outreach team, (3) a media and translation team, (4) a Telegram channel moderator team, and (5) a leadership team that pulls it all together. The teams likely consist largely of Ukrainian volunteers based in Ukraine, with a small fraction potentially living abroad. Particularly the media and Telegram channel moderator team might be open to foreigners, as no internal knowledge dissemination is necessary for these positions to be filled. It is also highly likely that the Ukrainian government is involved in the DDoS management of the IT Army, either through military conscripts, intelligence officers, or employees working for the Ministry of Digital Transformation.

The IT Army is highly responsive, nimble, quasi-transparent, and well-integrated into its surrounding ecosystem.

The share of DDoS traffic generated outside of Ukraine by the IT Army is likely multitudes higher than the DDoS traffic generated within Ukraine. One reason for this assessment is the IT Army's increasing reliance on abusing the services of large cloud service providers, including Amazon Web Service and Microsoft's Azure, to automatize and further centralize its DDoS campaigns. The IT Army essentially tasked its users to set up cloud instances and share the log-in credentials with the IT Army's Telegram bot. The IT Army's targeting team would then install DDoS tools on these cloud instances and centrally manage and synchronize the attacks.

The In-House Team

The second component of the IT Army is its in-house team. Initially, the team was defacing Russian websites to advertise the existence of the IT Army, and in some instance also to spread rumors on Russian domestic politics. In April 2022, the team ran an information warfare campaign against Russian soldiers that were sending boxes full of war loot home to their families from post offices in Belarus.[21] In the same month, the in-house team also released a video showing how they breached Russian Instagram clone Rossgram, and how they defaced the website of Sukhoi and Gazprom with statements attributed to their respective company's presidents criticizing the war.[22] In May 2022, the team ran their most destructive offensive cyberoperation to date, when they targeted the Russian video streaming platform RuTube.[23] The in-house team also breached electricity grid company

17 IT Army, "Чуєте," Telegram, July 5, 2023, https://t.me/itarmyofukraine2022/1349 or https://archive.ph/XNg8I

18 IT Army, "Хтось замовляв прогноз погоди," Telegram, July 20, 2023, https://t.me/itarmyofukraine2022/1430 or https://archive.ph/aBWlo

19 IT Army, "Beeline отримав," Telegram, July 1, 2023 https://t.me/itarmyofukraine2022/1338 or https://archive.ph/bEBl5

20 IT Army, "Рузський інтернет," Telegram, July 24, 2023, https://t.me/itarmyofukraine2022/1442 or https://archive.ph/cHgmM

21 IT Army of Ukraine, "Phone Call to Russian Looters," Youtube, April 6, 2022, https://youtu.be/d5ojdb9FyLY

22 IT Army of Ukraine, "Message to the citizens of Russia. What's happened to Rosgram?," Youtube, April 7, 2022, https://youtu.be/INyabM2IlG0; IT Army of Ukraine, "Miller is against the war, and Sukhoi lacks of details for aircraft — IT-army spreads the truth," Youtube, April 2022, https://youtu.be/1sfpTldvpPE

23 IT Army of Ukraine, "Взлом Rutube: самая большая победа кибервойны!" Youtube, May 14, 2022, https://youtu.be/pggg8sEDhjA

Loesk which potentially caused blackouts in the Leningrad Oblast.[24] The last publicly known campaign the in-house team has run targeted Gazprombank. According to Gazprombank president Alexander Egorkin, the attack was "*well done* [...] *done with fantasy*," as the team took out the website, the SMS provider [for two-factor authentication], and the call center at the same time.[25] Egorkin also elaborated that the in-house team "*knew the entire pool of bank IP addresses. All without exception, even those who were not involved in banking services*."[26] In contrast to the DDoS component of the IT Army, the in-house team's activities are never discussed in the Telegram channel nor on the IT Army's website. Instead, their activities are exclusively announced via videos on Youtube, which are then reposted on Telegram.

Once chosen, applicants have to complete a series of technical tasks to assess their skill levels, loyalty, and dedication to the Ukrainian cause.

Back in June 2022, CSS published the first and to-date only comprehensive analysis on the IT Army. Among other items, the report notes that "*it is highly questionable whether the Ministry of Digital Transformation has the legal authority to independently setup the IT Army and the Internet Forces without any coordination or control exercised by Ukraine's defense and intelligence services*."[27] In late-September 2022, Huib Modderkolk, investigative reporter for De Volkskrant, was able to interview a member of the inner circle of the IT Army in-person, known by the online handle Hactic. Hactic is not only living in the Netherlands, but is also a former Dutch Special Forces operator that joined the IT Army's management team in the early days. In the interview with Modderkolk, Hactic explains 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]."[28]

While we do not know how many members the in-house team has, we know a little bit about their recruitment process. On the DDoS side, anyone willing can participate in the IT Army's DDoS campaigns. There is no registration or approval process. By contrast, the in-house has a lengthy application process to prevent infiltrations. First, applicants have to fill out a Google docs form answering a multitude of questions such as, "*have you served in the military or intelligence agencies before*," "*how many years of experience do you have in pentesting*," and "*are you able to dedicate a minimum of 10 hours per week to IT ARMY*."[29] In March 2023, the IT Army, received more than 200 applications within a two-week period.[30] Once chosen, applicants have to complete a series of technical tasks to assess their skill levels, loyalty, and dedication to the Ukrainian cause. We do not know what happens afterwards. Applicants might become full members of a dedicated in-house team, or they could be left in limbo – receiving task after task without actually knowing what campaign they are part of.

24 IT Army of Ukraine, "Cyberattack on the Russian thermal power plant from the IT army of Ukraine," Youtube, October 15, 2022, https://youtu.be/1hIlRQF3brs

25 IT Army of Ukraine, "Газпром заценил атаку на себя. Привет от IT-армии Украины," Youtube, November 4, 2022, https://youtu.be/ED6V33bFluY

26 Ibid.

27 Stefan Soesanto, "The IT Army of Ukraine - Structure, Tasking, and Ecosystem," CSS/ETH, June 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf, p. 23

28 Huib Modderkolk, "Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol," De Volkskrant, September 24, 2022, https://www.volkskrant.nl/kijkverder/v/2022/een-internationaal-cyber-leger-tegen-rusland-met-een-nederlander-in-de-hoofdrol-v580287/

29 IT Army, "IT ARMY Volunteer Questionnaire," Google, March 14, 2022, https://web.archive.org/web/20230314164749/https://docs.google.com/forms/d/e/1FAIpQLSfdSnn52XhhkFPc3dQ-QKpifYyJU0Td8n0h9oYPeFHg2CM-vw/viewform

30 IT Army, "IT ARMY Volunteer Questionnaire," Google, n.d., https://web.archive.org/web/20230910104257/https://docs.google.com/forms/d/e/1FAIpQLSfdSnn52XhhkFPc3dQ-QKpifYyJU0Td8n0h9oYPeFHg2CM-vw/viewform

The Internet Forces of Ukraine

The Internet Forces of Ukraine were stood up on February 28, 2022, by the Ukrainian Ministry of Culture and Information Policy (MKIP) in cooperation with the Ministry of Digital Transformation.[31] Curiously, Western media have entirely ignored the conduct of the Internet Forces of Ukraine.[32] As of this writing, a Google search for the specific term "*Internet Forces of Ukraine*" shows a mere 244 results, while a search for the Ukrainian term "Інтернет Війська України" reveals 13.300 hits.

In contrast to the IT Army, the mission of the Internet Forces is to defend Ukraine's information front across all [Western] social media networks and traditional media outlets, by "*appeal*[ing] *to governments and influencers, refut*[ing] *fakes, ask*[ing] *for weapons from international partners, initiat*[ing] *petitions, encourage*[ing] *governments to impose an embargo on Russian oil, and* [pushing] *businesses to leave the Russian market*."[33] At its height, on March 15, 2022, the Telegram channel of the Internet Force of Ukraine counted 189.245 subscribers. As of this writing, it has 73.513 subscribers with an average loss rate of 1.613 subscribers per month.[34] The Internet Forces are also present on Instagram (as of this writing: 33.575 followers), Facebook (~30.000 followers) and Viber (6.615 members).[35] There is little to no interaction between the followers of the Internet Forces. All campaigns are centrally organized with no outside input.

It is highly likely that at some point in the past, the IT Army and the Internet Forces were envisioned to function as two sides of the same coin. The IT Army were to take out Russian media and government websites to (a) prevent the spread of Russian propaganda and (b) disrupt the daily lives of ordinary Russian citizen. While the Internet Forces would ensure that (c) the Ukrainian war narrative dominates in the [Western] information space, and (d) continuously seeps into Russian society at large. Yet, to date, the IT Army and the Internet Forces have never coordinated any of their campaigns. They work independently from each other with no known activity overlaps.

31 Oleksandr Tkachenko, "Міністерство культури та інформполітики й Мінцифра запрошують кожного приєднуватись до Інтернет Військ України," Telegram, February 28, 2022, https://t.me/otkachenkokyiv/1239 or https://archive.ph/zerzb; Міністерство культури та інформаційної політики України, "Міністерство культури та інформполітики запрошує кожного приєднуватись до Інтернет Війська України," Facebook, March 5, 2022, https://www.facebook.com/MCIPUkraine/posts/273889181561976 or https://archive.ph/SBNUn;

32 Вікторія Приседська, "Смартфон і планшет - теж зброя. Як українці воюють на віртуальному фронті," *BBC News*, March 11, 2022, https://www.bbc.com/ukrainian/features-60692128

33 Кабінет Міністрів України, "МКІП закликає всіх охочих долучитись до Інтернет військ, аби Україна залишалась у фокусі світових медіа," kmu.gov.ua, June 15, 2022, https://web.archive.org/web/20230720144624/https://www.kmu.gov.ua/news/mkip-zaklikaye-vsih-ohochih-doluchitis-do-internet-vijsk-abi-ukrayina-zalishalas-u-fokusi-svitovih-media

34 Tgstat, "Інтернет Війська України," n.d., https://web.archive.org/web/20230718084345/https://uk.tgstat.com/en/channel/@ivukr/stat

35 Інтернет Війська України, "ukrainian.internet.army," Instagram, n.d., https://instagram.com/ukrainian.internet.army; Інтернет Війська України, "Інтернет Війська України," Facebook, n.d., https://www.facebook.com/ukrainian.internet.army/; Інтернет Війська України, "ІНТЕРНЕТ ВІЙСЬКА УКРАЇНИ," Viber, n.d., https://vb.me/ivukr

Information Warfare Management

Due to its mission tasking, the Internet Forces ended up being an almost purely Ukrainian volunteer group. As Oleksander Tkachenko, the then Ministry of Culture and Information Policy, put it: "*now every civilian Ukrainian literally lives with a phone in his hands. So if you have access to the Internet and can spread information, the Internet of the Armed Forces of Ukraine is for you*."[36] According to a write-up on tsn.ua, the "the structure of the Internet Forces consists of a number of headquarters: designers' headquarters, copywriters' headquarters, assistants, and each of them is staffed by volunteers of the corresponding profile."[37] It is unclear where that information has been sourced from.

While it is unclear who exactly within the MKIP is controlling the Internet Forces, a strategic involvement by the Center for Strategic Communications and Information Security (Центру стратегічних комунікацій та інформаційної безпеки) – also known as Spravdi – seems inevitable. Founded in March 2021, Spravdi is part of the MKIP and specifically tasked to "*unite the efforts of civil society organizations and the government in the fight against disinformation, to respond quickly to fakes, and to promote Ukrainian narratives*."[38]

The Internet Forces have developed a standard campaigning format to rally its followers. For example, on September 29, 2022, the Internet Forces mobilized against the "*propaganda*" spread by "*some of the respectable foreign media*" that "*have begun to cover the results of 'referendums' that were illegally held in the territories occupied by Russia*."[39] To facilitate the campaign, the Internet Forces prepared several items: (a) two short paragraphs in English, (b) three accompanying images calling out Reuters, AFP, and the Financial Times, and (c) three lists with links to the social media accounts of 14 US, 17 German, and 20 French media executives and editors-in-chief.[40] The Internet Forces tasked its members to do two things: (1) post the paragraphs and pictures in the comments section of any social media posts of the accounts mentioned above, and (2) to make their own social media posts with the material provided. All instructions were posted in Ukrainian.[41] It is unknown how many people participated in this campaign. And it is unknown whether the campaign produced any discernible results as information warfare metrics are inherently difficult to grasp.

36 Oleksandr Tkachenko, "Міністерство культури та інформполітики й Мінцифра запрошують кожного приєднуватись до Інтернет Військ України," Telegram, February 28, 2022, https://t.me/otkachenkoky-iv/1239 or https://archive.ph/zerzb

37 TSN, "Інтернет-війська України: як стати частиною багатотисячного діджитал-війська," tsn.ua, April 13, 2022, https://tsn.ua/ato/internet-viyska-ukrayini-yak-stati-chastinoyu-bagatotisyachnogo-didzhital-viyska-2036344.html

38 Кабінет Міністрів України, Презентовано Центр стратегічних комунікацій та інформаційної безпеки," kmu.gov.ua, April 1, 2021, https://web.archive.org/web/20230720144807/https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki; Центр стратегічних комунікацій, "Про Центр," spravdi.gov.ua, n.d., https://spravdi.gov.ua/pro-nas/

39 Інтернет Війська України, "Друзі! Сьогодні ми знову боремося проти роспропаганди," Telegram, September 29, 2022, https://t.me/ivukr/1372 or https://archive.ph/nJgKV

40 Інтернет Війська України, "Reuters supports Terrorists by more than 96%," Telegram, September 29, 2022, https://t.me/ivukr/1373 or https://archive.ph/Elz0n; Інтернет Війська України, "Редактори видавництв," telegra.ph, March 16, 2022, https://telegra.ph/Redaktori-vidavnictv-03-16; Інтернет Війська України, "ЗМІ Франція," telegra.ph, March 17, 2022, https://telegra.ph/ZM%D0%86-Franc%D1%96ya-03-17; Інтернет Війська України, "ЗМІ Німеччини," telegra.ph, March 19, 2022, https://telegra.ph/ZM%D0%86-N%D1%96mechchini-03-19

41 The exception to this was an attempt by the Internet Forces to assemble an International Legion on Discord in March 2022. See: Інтернет Війська України, "Інтернет-військо, Допомога громадян західних країн важлива для перемоги, тому ми оголошуємо про створення іноземного легіону Інтернет Військ України," Telegram, March 26, 2022, https://t.me/ivukr/438 or https://archive.ph/LUuKH and Інтернет Війська України, "Become a Shield for Ukraine – Join Official Discord," Telegram, March 26, 2022, https://t.me/ivukr/439 or https://archive.ph/cAuaK; It is unclear to the author whether the Discord channel is still active.

Source: (left) The Internet Force's Telegram post on September 29, 2022; (center) Image created by the Internet Forces; (right) List of relevant social media accounts collected by the Internet Forces

Campaigning

On the one-year anniversary of the invasion, the Internet Forces summarized their activities as following: "*Together, we completed 459 tasks: banning businesses, signing petitions, attracting the attention of the international community, receiving weapons, and holding the information front. Thanks to your work, PayPal, McDonalds, Shell, Universal Music Group, Sony Music Entertainment, TOYOTA, Visa, Mastercard, etc. have withdrawn or suspended their business from Russia.* [...] *We have attracted the attention and support of world stars, including Jared Leto, Stephen King, Nassim Taleb, Michael Douglas, Benedict Cumberbatch, and Arnold Schwarzenegger*."[42] The Internet Forces also received congratulating video messages from several Ukrainian celebrities, including Natalka Denisenko, Kateryna Osadcha, and Julia Sanina.[43] While it is difficult to grasp the specific impact the Internet Forces had, one example may help gauge its significance: On August 11, 2022, the Latvian Parliament (Saeima) designated Russia as a "*state sponsor of terrorism*."[44] Anastasia Bondar, Deputy Minister for Culture and Information Policy subsequently stated on the MKIP website that, "*Ukraine is grateful to our friends from Latvia for their fair and honest vision of what today's Russia really is. The decision of the Latvian Saeima is a very good example of how coordinated joint actions help to win the information war. After all, every Ukrainian voice matters today. Therefore, join the Internet Forces of Ukraine and help the state to fight on the information front.*"[45] The website goes on to note that, "the Latvian Saeima's decision to recognize Russia as a state sponsor of terrorism is one of many successful tasks in which the Internet Forces have been integrated."[46]

42 Інтернет Війська України, "Сьогодні роковини нашої незламності, нашої боротьби, нашої сили," Telegram, February 24, 2023, https://t.me/ivukr/1758 or https://archive.ph/FXfKT

43 Інтернет Війська України, "Інтернет-військо, сьогодні з вами вітається наша українська акторка Наталка Денисенко. Впізнали? Так так, вона знімалась у фільмах «Століття Якова», «Кріпосна», а зараз записує відео для вас," Telegram, April 10, 2022, https://t.me/ivukr/600 or https://archive.ph/xjeAZ; Інтернет Війська України, "Інтернет-військо, Сьогодні Катерина Осадча закликає вас бути максимально активними!" Telegram, March 23, 2022, https://t.me/ivukr/399 or https://archive.ph/aNTdI; Інтернет Війська України, "Інтернет-військо, Юлія Саніна, фронтвумен гурту The HARDKISS передає вітання вам!" Telegram, March 22, 2022, https://t.me/ivukr/373 or https://archive.ph/OixQr

44 Latvian Republikas Saeima, "Saeima paziņojumā atzīst Krieviju par terorismu atbalstošu valsti," saeima.lv, August 11, 2022, https://web.archive.org/web/20230728140002/https://www.saeima.lv/lv/aktualitates/saeimas-zinas/31308-saeima-pazinojuma-atzist-krieviju-par-terorismu-atbalstosu-valsti

45 Міністерство культури та інформаційної політики України, "Інтернет Війська України в дії: сейм Латвії визнав Росію державою-спонсором тероризму," mkip.gov.ua, August 11, 2022, https://web.archive.org/web/20230720145918/https://mkip.gov.ua/news/7513.html

46 Міністерство культури та інформаційної політики України, "Інтернет Війська України в дії: сейм Латвії визнав Росію державою-спонсором тероризму," mkip.gov.ua, August 11, 2022, https://web.archive.org/web/20230720145918/https://mkip.gov.ua/news/7513.html

A comprehensive analysis of every campaign the Internet Forces have ever run – whether it is on sanction enforcement, urging Western weapon deliveries to Ukraine, demilitarizing the Zaporizhzhia Nuclear Power Plant, or pushing Russia out of the UN – will likely reveal specific coordinating patterns and distinctive relationships to non-governmental and state organizations both in and outside of Ukraine. As of this writing, no such comprehensive analysis currently exists.

One Internet Forces "campaign" might be of particular relevance when it comes to counter-hybrid warfare. Back in March 2022, the Internet Forces set up a Special Forces branch (Спецзагін) whose mission was to "*work undercover in the enemy's territory (VKontakte), break through the information blockade and bring the truth to the Russians*."[47] The Special Forces were assembled in their own Telegram channel, currently still 1.560 subscribers strong.[48] Members were supplied with a three-page step-by-step guide on how to conduct their operations, specialized software to automize their work, VKontakte group databases, text examples, and access to a Telegram bot that handed out the login credentials of existing VKontakte accounts. It is unknown who supplied the Internet Forces with the login credentials. They might have been bought from criminal marketplaces or could have been collected by the Ukrainian intelligence services. Essentially, members of the Special Forces used the supplied VKontakte accounts to post in hundreds of VKontakte groups and disseminate personal messages to its members. As the step-by-step guide put it, "*our priority now is to inform. All texts are written in such a way as not to provoke people into a dialog. That's why people rarely respond, and even then, it's not necessary to respond. It takes a lot of time and distracts from the main goal. If you have a desire to engage in a dialog and it really makes sense, we have a separate instruction for this case*."[49] The Internet Forces also explained that they "*monitor on a daily basis which narratives resonate most strongly in the minds of Russians and lead to the gradual destabilization of the social situation in the aggressor country*."[50] It is unknown whether or how successful the Special Forces have been on VKontakte. No new messages have been posted in the Special Forces Telegram channel since April 13, 2022.[51]

Overall, the Internet Forces are a mixture of supporting Ukrainian government pressure on Western governments, calling out individual companies for their continued business in Russia, and creating new propaganda narratives geared to dismantle any potential for rapprochement with the Russian state.

47 Інтернет Війська України, "В лавах Інтернет Військ України ми оголошуємо набір в Спецзагін, що буде працювати під прикриттям на території ворога - у ВКонтакті," Telegram, March 24, 2022, https://t.me/ivukr/402; Спецзагін ІВУ | Підготовка, "Спецзагін Інтернет Військ України," google.com, n.d., https://docs.google.com/document/d/1C6W93xSCKanCWaLcut04hVI-flvlQtPceCpMeKirZOY/edit?usp=sharing or https://archive.ph/0uGw1

48 Спецзагін | Інтернет Війська України, "Особливий підрозділ Інтернет Військ України, який працює під прикриттям на території ворога - в ВКонтакті," Telegram, n.d., https://t.me/+vtoYYtjogFliODZi or https://archive.ph/yimFu

49 Інтернет Війська України, "В лавах Інтернет Військ України ми оголошуємо набір в Спецзагін, що буде працювати під прикриттям на території ворога - у ВКонтакті," Telegram, March 24, 2022, https://t.me/ivukr/402; Спецзагін ІВУ | Підготовка, "Спецзагін Інтернет Військ України," google.com, n.d., https://docs.google.com/document/d/1C6W93xSCKanCWaLcut04hVI-flvlQtPceCpMeKirZOY/edit?usp=sharing or https://archive.ph/0uGw1

50 Інтернет Війська України, "В лавах Інтернет Військ України ми оголошуємо набір в Спецзагін, що буде працювати під прикриттям на території ворога - у ВКонтакті," Telegram, March 24, 2022, https://t.me/ivukr/402; Спецзагін ІВУ | Підготовка, "Спецзагін Інтернет Військ України," google.com, n.d., https://docs.google.com/document/d/1C6W93xSCKanCWaLcut04hVI-flvlQtPceCpMeKirZOY/edit?usp=sharing or https://archive.ph/0uGw1

51 Спецзагін | Інтернет Війська України, "Особливий підрозділ Інтернет Військ України, який працює під прикриттям на території ворога - в ВКонтакті," Telegram, n.d., https://t.me/+vtoYYtjogFliODZi or https://archive.ph/yimFu

Lessons Learned

Both the IT Army and the Internet Forces are government-created and government-managed volunteer efforts that emerged in reaction to the Russian invasion of Ukraine. As of this writing, a handful of lessons learned can be extracted:

Both the IT Army and the Internet Forces [...] emerged in reaction to the Russian invasion of Ukraine.

1. **Legality:** Depending on one's political point of view, the IT Army either operates in a very very gray space or is committing clear violations under international law. Particularly problematic, is (a) the targeting of Russian civilian infrastructure in cyberspace, (b) the tasking of people living in non-belligerent countries across the globe to participate in these campaigns, (c) the utilization of Western cloud and VPN infrastructures to enable these operations and (d) the spread of DDoS tools to anyone interested which might spur the conduct of cybercrime.
2. **Gamification:** Repetitive tasking is the major reason why volunteers are leaving the IT Army and the Internet Forces. Gamification could be utilized to break the dullness. Yet, to date, neither the IT Army nor the Internet Forces have had much success in finding viable gamification methods that are both scalable and attention grabbing to stem the steady outflow of volunteers.
3. **Reach:** An online volunteer force needs to have a global reach, or at a minimum a regional one. The Internet Forces' Ukraine-only approach severely limits the size of the group, its ability to conduct country specific operations, and it weakens innovation pressures.
4. **Communication:** While engaging with one's user base is a must, oversharing seems to be rather detrimental to the overall cause. Instead, quasi-transparency and keeping internal deliberations hidden from the public are the way to go to avoid infighting, faction-building, and drama.
5. **Language:** Even though translation services are easily available online, communicating in English is a must to connect with a global audience. A multilingual approach in English, Ukrainian, and potentially a third language seems to be the way to go. If feasible, current automatic translations ought to be avoided, and instead native speakers ought to be used to better connect with once audience. AI chatbots and automation will likely fill this void in the future.
6. **Platforms:** A presence on multiple social media platform is largely counter-productive as it substantially increases the media team's workload, fosters community splintering, and makes direct interaction with members more difficult.
7. **Government connection:** Without the involvement and public endorsement of government agencies, neither the IT Army nor the Internet Forces would have grown as fast as fast as they did. The Ministry of Digital Transformation has done an outstanding job in promoting the IT Army and turning it mainstream. By contrast, the Ministry of Culture and Information Policy has done a rather poor job.
8. **Evolutionary trajectory:** Constant evolution is a must. Members have to feel that the group is making progress in both substance and thinking. These can include the release of new tools, website overhauls, new media strategies, special campaigns etc.

As of this writing it is unclear whether the success of the IT Army and Internet Forces can be replicated under different conditions. The paper has outlined how both groups are internally organized, how they conduct their campaigns, how they are incorporating volunteers from abroad and at home, and how these two groups are linked to the Ukrainian government. The paper has tried to contextualize their discernible impact, resulting questions for the law of armed conflict, and highlighted some lessons learned that might help in replicating their efforts. Time will tell whether the IT Army and the Internet Forces groups will serve as blueprints for others to evolve upon, or whether they will remain unique in their own right.

Repetitive tasking is the major reason why volunteers are leaving the IT Army and the Internet Forces. Gamification could be utilized to break the dullness.

Stefan Soesanto is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich. He leads the Cyberdefense Project and is the Co-Team Head of the Risk and Resilience Team. Prior to joining CSS, he was the Cybersecurity & Defense Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum CSIS. Stefan also served as a Research Assistant at RAND's Brussels office, co-authoring reports for the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Network Information Security Agency (ENISA), and Dutch Ministry of Security and Justice. Stefan holds an MA from Yonsei University (South Korea) with a focus on security policies, and international law, and a BA from the Ruhr-University Bochum (Germany) in political science and Japanese.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl