The IT Army of Ukraine

Structure, Tasking, and Eco-System

CYBERDEFENSE REPORT

The IT Army of Ukraine
Structure, Tasking, and Ecosystem

Stefan Soesanto

Zürich, June 2022
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at:
css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Stefan Soesanto

ETH-CSS project management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andrin Hauri, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editor: Taylor Grossman
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000552293

Table of Content

1	**Introduction**	**4**
Research Methodology		5
2	**Genesis**	**6**
How many members does the IT Army have?		7
3	**Targeting Flow and Coordination**	**8**
Simple Tasking		8
Target Enrichment		9
External Clustering		10
Ad Hoc Prioritization		10
IT Army Coordination Document		11
GitHub Repositories		13
4	**Hacken, Liberator, and Hackenproof**	**15**
5	**Non-public Structure and Tasks**	**19**
6	**Where are Ukraine's intel services?**	**23**
7	**The IT Army and External Groups**	**25**
Anonymous		25
Belarusian Cyber Partisans		27
IPStress		27
8	**Conclusion**	**28**
List of Acronyms		**30**
About the Author		**31**

1 Introduction

For several years prior to the Russian invasion on 24 February 2022, the principal idea of creating a cyber volunteer army had been bouncing around in Ukrainian government circles. In part, those discussions were informed by the success of the Estonian Defence League's Cyber Unit and other efforts around the globe to organize, incorporate, and surge civilian IT volunteers into existing military structures in times of need.

In contrast to these well-established and purely defensive cyber volunteering efforts, the IT Army of Ukraine was stood up in an ad-hoc manner without a clearly structured and proven plan. Similarly, the absence of a Ukrainian military cyber command likely also pushed Kyiv to think creatively about how to combine its nascent military and intelligence cyber capabilities with a massive, willing, and global civilian IT community in the defense of the nation. Born out of necessity, the IT Army subsequently evolved into a hybrid construct that is neither civilian nor military, neither public nor private, neither local nor international, and neither lawful nor unlawful.

As of this writing, the IT Army consists of two parts: (1) a continuous global call to action that mobilizes anyone willing to participate in coordinated DDoS attacks against designated – primarily civilian – Russian infrastructure targets; and (2) an in-house team likely consisting of Ukrainian defense and intelligence personnel that have been experimenting with and conducting ever-more complex cyber operations against specific Russian targets. Both parts of the IT Army are purely offensive in nature and serve to bring willing amateurs (civilians) and dedicated professionals (civilian, military, intel) into one – most likely – hierarchically organizational structure.
In addition, the IT Army has also given rise to an ecosystem that includes Ukrainian-owned IT companies and individuals located outside of Ukraine, as well as Ukrainians living in Ukraine working for Western companies. This ecosystem has been continuously creating new tools, generating knowhow, identifying new targets, and fulfilling other intelligence support functions to underpin Ukraine's offensive efforts in cyberspace.

Who needs a military cyber command when you have the IT Army?

The IT Army's structure and gravitational pull has created a myriad of new problem sets for the international community in areas such as the application of international law in cyberspace, the normative behavior of states, the targeting of civilian infrastructure, and the ethical conduct of IT companies headquartered outside Ukraine, to name a few. Many – if not all – of these problem sets have been largely ignored by the academic and information security community, as well as policymakers in both EU and NATO member states. It is unclear why this is the case, but it seems that the political and ideological support for the defense of Ukraine on the one hand, and growing anti-Russian sentiments on the other, have created an environment in which Ukrainian conduct in cyberspace is either willfully ignored, superficially analyzed, or significantly downplayed in terms of its impact and relevance.

On the DDoS side, the IT Army's conduct shares a wide array of strategic overlaps with the DDoS campaign against Estonia in May 2007. The 2007 campaign was organized by Russian nationalistic hacktivists via Russian language fora / websites and lasted 22 days. To this day, no clear evidence of Russian government involvement has emerged, and as such the campaign was never officially attributed to the Russian state. As a result, Estonian and Western criticism pivoted to point out that Moscow had taken no meaningful measures to mitigate the DDoS campaign (a violation of its due diligence obligation), and the lack of cooperation with the Estonian investigation was highlighted as proof that the Russian government is shielding – and thereby implicitly supporting – those responsible for the DDoS campaign. Amidst this environment of helplessness, the speaker of the Estonian Parliament Ene Ergma even famously stated that, "when I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing".[1]

Yet, in contrast to 2007, the IT Army's DDoS conduct is pretty clear-cut when it comes to attribution, government authority, instructions, direction, and control. It is similarly clear-cut that the IT Army is persistently and indiscriminately targeting Russian civilian infrastructure, including online pharmacies, banks, food delivery services, and retailers. But while Russia has been rightfully vilified for the DDoS attacks in 2007, the IT Army and its Minister of Digital Transformation Mykhailo Federov received two awards at the CYBERSEC European Cybersecurity Forum 2022 in Katowice, Poland, for their "heroic resistance to Russian aggression and protection of the digital borders

[1] Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack," *Wired*, 22 August 2007, https://www.wired.com/2007/08/cyber-war-and-e/.

of the democratic world".[2] As Federov put it, "this award is first and foremost for the entire cyber community and the volunteers who are now waging the world's first cyberwar with us".[3] While there is certainly a difference between DDoS campaigns conducted in peacetime and during times of war, it seems that the West is now throwing overboard the legal and normative interpretations it has championed in cyberspace over the past decade for the sake of politically supporting Ukraine.

On the in-house side, the IT Army's conduct has rapidly evolved from mere defacements of Russian websites during the first days of the invasion, to sophisticated espionage campaigns, to the first destructive offensive cyber operation – targeting a civilian video platform – in early May 2022. Currently, it is unclear what kind of cyber operations the in-house team side is going to focus on in the future. But, if the evolutionary trajectory over the past 4 months is any metric to go by, Russian defenders will highly likely face a variety of experimental cyber ops that will try to produce more and more severe impacts and longer lasting effects. Considering this trajectory, it is particularly curious to witness that a group of human rights lawyers recently decided to push the International Criminal Court in The Hague to open the first ever cyberwar crime case against Sandworm – a Russian military intelligence unit that successfully targeted electric utilities in Ukraine and caused short regional blackouts back in 2015-16.[4]

Research Methodology

The overarching aim of this report is to provide a comprehensive study that will serve as a baseline to understand, assess, and analyze the conduct of the IT Army and the ecosystem that feeds it.

As such, this report was compiled by using only publicly accessible data. This includes public websites, Twitter posts, media articles, interviews, podcasts, Youtube videos, GoogleDoc forms, as well as hundreds of Telegram channels and chats. At no point during this research endeavor did the author participate in any of the malicious or illegal cyber activities mentioned in this report.

Joining and reading hundreds of Telegram channels and chats was of particular importance for accessing and contextualizing the detailed information included in this report. For example, Telegram's search function allows researchers to crawl through every channel they subscribe to and every chat they are a member of. This function was particularly helpful for tracking specific terms, targets, URLs, IPs, and port numbers across multiple Telegram channels and chat: The more channels and chats one has joined, the more visibility one has on the platform. The search function also chronologically displays the search hits which makes tracking information back to their likely origin a lot easier.

Please note that joining a Telegram channel or chat does not constitute any formal membership, nor did it impose any obligations – financial, political, or otherwise – on the author.
Joining a Telegram channel makes one a subscriber, thus, for example, enabling the option to set up new post alerts. One can also join a Telegram chat – which makes one a member of that chat – and enables the option to write in the chat. While most channels and chats can be viewed without joining, some channels and chats do prevent non-subscribers and non-members from seeing their content. A small number of subscriptions also require the confirmation of a channel administrator. Usually, these are granted within minutes and are only imposed to exercise a limited form of user admission control. In particular, Russian hacking groups are using this process to root out pro-Ukraine users.

During this research, the author did not post in any of the Telegram channels and chats. Nor did he engage in any private conversations with any Telegram users across the multitudes of channels and chats. The author did talk to several hacking groups on Twitter that have claimed to cooperate with the IT Army. Yet, none of these claims could be confirmed – and subsequently do not appear in this report – due to the IT Army's unresponsiveness to the author's email inquiries.

In terms of the report's limitations, two items ought to be highlighted. First, the author did not have perfect visibility into all the relevant hacking communities on Telegram, as he was likely not a member of every pertinent Telegram channel and chat. It is thus unclear whether there were any other information flows occurring on Telegram that this report was unable to capture. Second, specific posts in Telegram chats are unlinkable by their very nature, and access to a good number of chats is usually granted through time-limited public invitations. As a result, this

[2] The Odessa Journal, "Ukraine received two awards in the field of cybersecurity at the CYBERSEC European Cybersecurity Forum," *Odessa-journal*, 18 May 2022, https://web.archive.org/web/20220608141159/https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-the-cybersec-european-cybersecurity-forum/.

[3] Ibid.

[4] Andy Greenberg, "The Case for War Crimes Charges Against Russia's Sandworm Hackers," *Wired*, 12 May 2022, https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/.

report is unable to provide functioning URLs to most of the chats and is unable to provide specific URLs to reference distinct Telegram chat posts. Wherever possible Telegram links are archived using archive[.]ph and non-Telegram links are archived via the Wayback Machine.

2 Genesis

The creation of the IT Army of Ukraine (IT-армія україни) begins with Yegor Aushev. Aushev is a well-known Ukrainian IT entrepreneur and the co-founder of three companies that have become increasingly relevant amidst the eight year-long war with Russia – Cyber Unit Tech, Cyber School, and Hacken.io. Sometime between 24 February (the day of the Russian invasion) and 26 February, Aushev pitched the idea of a cyber volunteer army to Mykhailo Federov, Ukraine's 31-year-young Minister of Digital Transformation.[5]

Around the same time, Aushev also embarked on assembling a 1,000-men strong Ukrainian cybersecurity volunteer group at the request of a senior Ukrainian Defense Ministry official.[6] Aushev facilitated the latter on Twitter and in various hacking fora by posting a Google Docs application form to gauge an applicant's skill level and area of expertise.[7] According to Aushev, this group of around 1,000 Ukrainian cybersecurity volunteers would be divided into an offensive and a defensive group. Talking to Reuters on 24 February, Aushev elaborated that the defensive group will be "employed to defend infrastructure such as power plants and water systems," and the offensive group would help "Ukraine's military conduct digital espionage operations against invading Russian forces". As Aushev put it, "we have an army inside our country. […] We need to know what they are doing".[8] As of this writing, the ratio between these two groups is still unknown.

Inspired by Aushev's idea of an army of cyber-volunteers, Federov took to Facebook on 26 February at 9.00 a.m. CET and posted the following message in Ukrainian: "We have a lot of talented Ukrainians in the digital sphere: developers, cyberspecialists, designers, copywriters, marketers, targetologists, etc. We are creating an IT army. All operational tasks will be presented in the telegram channel: t.me/itarmyofurraine. There will be tasks for everyone".[9] Federov posted the same message in Ukrainian on his verified 170,000 subscriber strong Telegram channel.[10] And at 7.38 p.m. CET his verified Twitter account tweeted in English that: "We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine".[11]

Western media coverage on the birth of the IT Army has almost exclusively focused on Federov's Twitter post – because it was written in English – and ignored his Facebook and Telegram ones.[12] But there are curious differences between these three posts. First, Federov's target audience on Twitter was clearly international, while on Facebook and Telegram it was primarily aimed at Ukrainians. Second, in his Facebook and Telegram posts Federov was very precise about the exact talent the IT Army sought. And third, in all three messages Federov misspelled "ukraine" – but only his Telegram post was later corrected. Funnily enough, because of this mishap, there is only one post in the "itarmyofurraine" channel which redirects users to the official and correct "itarmyukraine2022" channel. Curiously, someone also decided to open up a Telegram channel on the same day, named "itarmyofuraine" (one "r," missing "k"), which currently has around 11,500 subscribers and reposts some of the content from the official channel.[13] Probably most crucial, western media outlets missed a post by the official Telegram channel of the Ministry of Digital Transformation on 26 February at 6.48 p.m. CET. Its content was almost identical to Federov's recruitment message, except the Ministry added one crucial sentence: "we urge you to use any vector of cyber and DDoS attacks on Russian resources".[14] This call to arms echoed the first ever

[5] See also: Adam Janofsky, "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites," *The Record*, 4 March 2022, https://web.archive.org/web/20220608141213/https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/.

[6] Joel Schectman and Christopher Bing, "EXCLUSIVE Ukraine calls on hacker underground to defend against Russia," *Reuters*, 24 February 2022, https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

[7] Graham Cluley, "Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces," *Bitdefender*, 25 February 2022, https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/.

[8] Joel Schectman and Christopher Bing, "EXCLUSIVE Ukraine calls on hacker underground to defend against Russia," *Reuters*, 24 February 2022, https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

[9] Mykhailo Federov, Facebook, 26 February 2022, https://www.facebook.com/mykhailofedorov.com.ua/posts/1005386320078887.

[10] Mykhailo Federov, Telegram channel, 26 February 2022, https://t.me/zedigital/1114 or https://archive.ph/H2caw.

[11] Mykhailo Federov, Twitter, 26 February 2022, https://web.archive.org/web/20220226232059/https://twitter.com/FedorovMykhailo/status/1497642156076511233.

[12] For example, *Wired* linked to Federov's Facebook post, see: Tom Simonite and Gian M. Volpicelli, "Ukraine's Digital Ministry is a Formidable War Machine," *Wired*, 17 March 2022, https://www.wired.com/story/ukraine-digital-ministry-war/.

[13] The description of both the official IT Army channel and the itarmyofuraine includes the official IT Army of Ukraine email (itarmyua@gmail.com).

[14] Ministry of Digital Transformation, Telegram Channel, 26 February 2022, https://t.me/mintsyfra/2609 or https://archive.ph/7UYkx.

post in the official IT Army Telegram channel, which proclaimed two hours earlier: "Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources". The post then listed 31 Russian banks, businesses, and government websites.[15]

As of this writing it is unknown what exactly sparked the internal shift away from assembling developers, designers, and copywriters toward the IT Army's almost sole focus on DDoS attacks. One likely explanation is that the specific Ukrainian talent that Federov outlined in his post was in the end funneled into a group called "StandForUkraine". StandForUkraine was stood up by Roman Zakharov, a 37-year-old Ukrainian IT executive. The group currently consists of around 1,300 "software engineers, marketing managers, graphic designers and online ad buyers" that are fighting on Ukraine's information warfare front.[16] The group is trying to mobilize non-Ukrainians and the international community against the Russian invasion and is spreading Ukrainian war propaganda across Western media outlets and social media platforms. The group has also successfully pushed Western companies out of Russia.[17] StandForUkraine has its own website, but in contrast to the IT Army, it is only using invite-only private chats on the messaging app Signal to communicate and organize. Future CSS research mights take a deep dive into the StandForUkraine ecosystem.

For the IT Army, it is important to stress that Federov is very active on Telegram but has only posted on Twitter 500 times or so since November 2020. Yet, even on Telegram, Federov rarely talks about the IT Army. Between 26 February and 20 April, he only forwarded 18 messages from the official IT Army channel. For a minister who created this digital army of volunteers, Federov seems rather disinterested in it. Instead, most of his Telegram posts gravitate toward his efforts to push Western companies out of Russia, fundraise for humanitarian projects and the Ukrainian armed forces, and inform citizens about the latest work of his Ministry.

One might assume the website of the Ministry of Digital Transformation would prominently display its connection to the IT Army and cover its ongoing activities in some way, shape, or form.[18] And one would be wrong. As of this writing, there is not a single news item on the Ministry's website that talks about the IT Army. Similarly, the Ministry's official Telegram channel has mentioned the IT Army a mere ten times and forwarded just four posts from the official IT Army channel between 26 February and 20 April.[19] Possibly spurred by the lack of consistent coverage, the Ministry's Telegram channel announced on 18 April that moving forward, on every Monday it will talk about the victories of the IT Army.[20] Notably, on 23 May, the Ministry summarized that "since the Russian invasion of Ukraine, the IT army has attacked about 2,000 Russian resources".[21]

Curiously, the Ministry did mention the IT Army and its Telegram channel in two news items on kmu.gov.ua – the official web portal of the Ukrainian government – more than two weeks after Federov's recruitment call. A news item on 10 March briefly acknowledged the existence of the IT Army, while the 12 March post prominently headlined, "the Ministry of Digital Transformation has created 3 services to fight the occupiers on the digital front": The IT Army, the Internet Forces of Ukraine, and the e-Enemy app "eBopor".[22]

The uneven and rather bumpy IT Army coverage by the Ministry of Digital Transformation in the first two months after the invasion might be an outcome of the diffuse and still evolving organizational structure of the IT Army itself.

How many members does the IT Army have?

Public reporting has put the number of IT Army members at around 300,000, which is derived from the number of subscribers to the official IT Army Telegram channel.[23] According to TGStat, a platform that provides analytics for

---

[15] IT Army of Ukraine, Telegram channel, 26 February 2022, https://t.me/itarmyofukraine2022/1 or https://archive.ph/SMt31.

[16] Frank Bajak, "Ukraine digital army brews cyberattacks, intel and infowar," *Associated Press*, 5 March 2022, https://web.archive.org/web/20220608141931/https://apnews.com/article/russia-ukraine-technology-europe-hacking-f2c4960e48b8022a567780f3602b54e2.

[17] Ibid.

[18] Website of the Ministry of Digital Transformation Ukraine, https://thedigital.gov.ua/; Telegram channel of the Ministry of Digital Transformation, https://t.me/mintsyfra.

[19] Ministy of Digital Transformation, Telegram channel, search query "IT Army" and "IT-армію," https://t.me/s/mintsyfra?q=%D0%86%D0%A2-%D0%B0%D1%80%D0%BC%D1%96%D1%8E; https://t.me/s/mintsyfra?q=it+army.

[20] Ministy of Digital Transformation, Telegram channel, 18 April 2022, https://t.me/mintsyfra/2921 or https://archive.ph/rDwiT.

[21] Ministy of Digital Transformation, Telegram channel, 23 May 2022, https://t.me/mintsyfra/3065 or https://archive.ph/qJk5P.

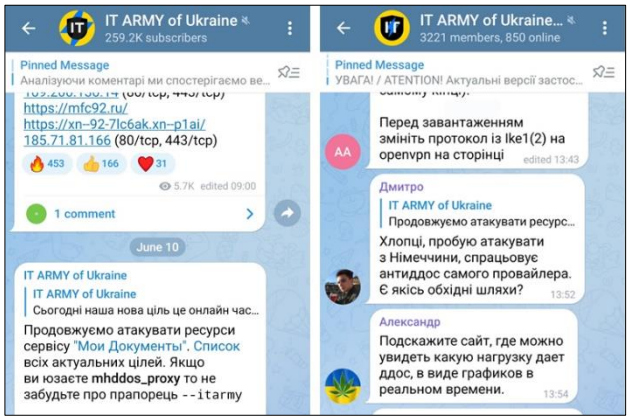
[22] KMU.gov.ua, "Мінцифри бореться з ворогом на цифровому фронті," March 10, 2022, https://web.archive.org/web/20220310141242/https://www.kmu.gov.ua/news/mincifri-boretsya-z-vorogom-na-cifrovomu-fronti; KMU.gov.ua, "Мінцифри створило 3 сервіси, щоб боротися з окупантами на цифровому фронті," 12 March 2022, https://web.archive.org/web/20220313185053/https://www.kmu.gov.ua/news/mincifri-stvorilo-3-servisi-shchob-borotisya-z-okupantami-na-cifrovomu-fronti.

[23] Chris Stokel-Walker and Dan Milmo, "'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia," *The Guardian*, 15 March 2022, https://web.archive.org/web/20220608145557/https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia; Corin Faife, "In Ukraine, Hacktivists fight back with Data Leaks," *The Verge*, 11 March 2022, https://web.archive.org/web/20220608145521/https://www.thev-

Telegram channels and chats, the IT Army's Telegram channel reached its highest subscriber count on 26 March with 307,165.[24] From thereon out, the numbers have continuously trended downward, leading to a cumulative loss of 47,940 subscribers over the following eight weeks (15.6%). On 10 June, the IT Army subscriber count stood at 259,225.[25]

While it is unknown why exactly the channel has been losing so many followers so quickly, the likeliest explanation is probably a combination of (1) the loss of novelty over time, (2) boredom due to repetitive tasking, and (3) the ongoing kinetic war itself, which remains largely unaffected by the IT Army's DDoS activities due to the focus on targeting Russian civilian infrastructure.

To contextualize the IT Army's subscriber number it is useful to know that Telegram offers two platform types: (a) channels in which only the channel administrator's messages appear, and users can comment if that function is enbled. And (b) chats where users can actually have somewhat of a dialogue with multiple members.



June 10, 2022, screenshots of the IT Army channel (left) and chat (right)

In the IT Army's Telegram channel – which is literally open to anyone – there is little to no in-depth operational discussion taking place. The IT Army also has an official Telegram chat, yet its number stands at a mere 3,200 members. Discussion in the chat primarily gravitates toward helping other members solve their technical problems, and occasionally highlighting new potential Russian targets that are worth DDoSing.

So, how many members does the IT Army really have? Nobody actually knows, not even the IT Army itself. What the IT Army does know – or more precisely put – what the IT Army's coordination team and Telegram channel administrators know, is the exact number of people that have directly approached them to offer their skills and time via the IT Army's Gmail account and Google Docs contact forms.[26] As of this writing, that number has not been publicly disclosed.

3 Targeting Flow and Coordination

What we do know is that the IT Army's Telegram channel is just one component within the IT Army's organizational structure – essentially serving as a sort of megaphone to circulate DDoS targeting information.[27] In an interview with Ukrainian outlet *Media Sapiens* in late March, Mstislav Banik, the Head of the Electronic Services Development at the Ministry of Digital Transformation explained that "all tasks are formed by channel curators, who distribute them in the channel for volunteers. Anyone can subscribe to the project's telegram channel and receive assignments".[28]
With the aid of a few practical examples the following paragraphs will explain how the visible part of this targeting flow works in practice.

Simple Tasking

The first example is on "simple tasking". Here, the exact same targeting information the IT Army channel publishes is circulated in numerous other channels and chats. On 18 March at 3.50 p.m. CET, the IT Army channel posted the

erge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cyber-crime-danger; Elise Labott, "'We Are the First in the World to Introduce This New Warfare': Ukraine's Digital Battle Against Russia," *Politico*, 8 March 2022, https://web.archive.org/web/20220608135145/https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880.

[24] TGStat, "IT Army of Ukraine – Subscribers number growth," n.d., https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers.

[25] Ibid.

[26] IT Army, "IT Army," Google Docs, accessed in March or April, https://web.archive.org/web/20220509133343/https://docs.google.com/forms/d/e/1FAIpQLSfeFKKXQkQaZDwVPZQVRSvbETYtsVZXBawF7fawHeC-m4mQZw/viewform; IT Army, "Offer help," Google Docs, accessed in March or April, https://web.archive.org/web/20220509133603/https://docs.google.com/forms/d/e/1FAIpQLSe3M1jW5ieBkd4FMpktrFuRpCpmF5zQjg8W1qHe9uO0z_QO-g/viewform

[27] For an evaluation of the impact of the DDoS attacks see: Chris Partridge, "ru-ok," Github, https://web.archive.org/web/20220608112818/https://github.com/tweedge/ru-ok; Kyle Alspach, "Ukraine's IT army is doing well, hitting Russia with 'cost and chaos'," *VentureBeat*, 4 March 2022, https://web.archive.org/web/20220608145845/https://venturebeat.com/2022/03/04/ukraines-it-army-is-doing-well-hitting-russia-with-cost-and-chaos/.

[28] Ira Ryaboshtan, "Мстислав Банік, Мінцифри: Західні компанії не мають ставати спонсорами російського вторгнення та загибелі українців," *Media Sapens*, 23 March 2022, https://web.archive.org/web/20220608112712/https://ms.detector.media/internet/post/29223/2022-03-23-mstyslav-banik-mintsyfry-zakhidni-kompanii-ne-mayut-stavaty-sponsoramy-rosiyskogo-vtorgnennya-ta-zagybeli-ukraintsiv/.

URL of vesti95[.]ru, one of vesti95's IPs, and four ports. *Vesti95* is the official newspaper published by the Ministry of the Chechen Republic for National Policy, External Relations, Press and Information. A mere three minutes later the same information appeared in a chat named "DDoS Joint Group" (around 1,900 members). 20 minutes after that, it was published in the "Hacker Forces" channel (around 1,100 subscribers), which is the official channel of Hacken.io's volunteer cyber army. Hacker Forces kindly credited the source of the information by explaining that, "here is a new task from itarmyofukraine2022. Are you in?"[29] At 5.39 p.m., a channel called "Studentcyberarmy" (around 900 subscribers) posted the exact same information with no credit to the IT Army, and literally within the same minute that information was forwarded in the "CyberFire" chat (around 5,500 members).[30] At 7.00 p.m., a channel belonging to "Cyber Palyanitsa" (around 700 subscribers) posted the same targeting details with no credit given.[31] And at 7.59 p.m. CET, the information popped up on the "disBalancer Ukraine" channel (around 5,500 members), which is the Ukrainian channel of Hacken.io's disBalancer DDoS tool.[32] On 20 March at 4.16 p.m. CET, the "disBalancer English" channel (around 13,500 members) posted the url of vesti[.]ru under the header of "Websites [that] were under attack on 18 March 2022".[33] One hour later that post was forwarded in the Hacker Forces channel.[34] As this example shows, Hacken.io is deeply entrenched in the information flow coming out of the IT Army channel. This should not come as a surprise, given that Aushev was the co-founder of Hacken.io. But the relationship between the IT Army and Hacken.io runs much deeper than that – more on this later.

Date & Time	Channel or Chat	Targeting Information Shared
18-Mar, 15:50	IT Army of Ukraine channel	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 15:50	IT Army of Ukraine chat	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 16:13	Hacker Forces channel	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 17:39	Studentcyberarmy channel	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 17:39	CyberFire chat	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 19:00	Cyber Palyanitsa Channel	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
18-Mar, 19:59	disBalancer Ukraine chanel	91.106.207.34 21/TCP, 22/TCP, 80/TCP, 3306/TCP
20-Mar, 16:16	disBalancer channel	Vesti95.ru
20-Mar, 17:16	Hacker Forces channel	Vesti95.ru

Target Enrichment

The second example is on what is best described as "target enrichment." Here, the targeting information posted by the IT Army channel is only circulated when it is further enriched with more IPs and ports. On 14 March at 9.11 a.m. CET, the IT Army channel posted the url of asna[.]ru and one of its IPs. Asna represents a network of more than 10,000 pharmacies in Russia and its website functions as a nationwide online pharmacy. The IT Army's targeting information was only re-published in the DDoS Joint Group chat and a channel called "KiberBull" (around 7,800 subscribers), but no other channel or chat visible to me.[35] That calculus changed eight days later when on 22 March at 10.38 a.m. CET, the Studentcyberarmy announced, "Good morning, today we start our day on the cyber front with a store in the pharmaceutical industry, namely ASNA! We are attacking until 13:00!"[36] Included in the post was the IP mentioned by the IT Army, two additional target IPs, and six ports – two for each of the three IPs. One minute later that post was forwarded to the CyberFire chat and the "DDoS Attack Cyber Cossacks" chat (around 25,800 members). At 10.51 a.m. CET the "Cyber Cerber" chat (around 600 members) posted the exact same targeting information with no credit given, and at 11.35 a.m. the "DDoS Attack Cyber Cossacks" channel (around 69,800 subscribers) tasked its DDoS teams one and four to hit the three Asna IPs. Each Cyber Cossacks DDoS team has about 1,000 dedicated members who are highly active and coordinate their activities in their own separate chats. On the next day at 12.08 p.m. CET, Cyber Palyanitsa posted the same targeting information again. Nine minutes later it appeared in the Cyber Cerber chat, and eight minutes after that it was reposted in a channel called "Anonymous-Ukraine" (around 1,900 subscribers).[37] At exactly 12.29 p.m. CET, the Studentcyberarmy made a new post with the same Asna targeting information, which was immediately forwarded in the CyberFire chat. Seven minutes later, the DDoS Attack Cyber Cossacks channel posted the commands to pull the latest docker image to update the target information for

[29] Hacker Forces, Telegram channel, 18 March 2022, https://t.me/hackencyberarmy/101 or https://archive.ph/ILjlY.

[30] Studentcyberarmy, Telegram channel, 18 March 2022, https://t.me/studentcyberarmy/193 or https://archive.ph/mfXYH; CyberFire Chat, Telegram channel, 18 March 2022, https://t.me/cyberfirechatt/52321 or https://archive.ph/niCZo.

[31] CyberPalyanitsa, Telegram channel, 18 March 2022, https://t.me/CyberPalyanitsa/215 or https://archive.ph/ZKCBq.

[32] disBalancer Ukraine, Telegram chat, 18 March 2022, https://t.me/c/1701910482/50239.

[33] disBalancer English, Telegram channel, 20 March 2022, https://t.me/disbalancer_group/113188 or https://archive.ph/dBWON.

[34] Hacker Forces, Telegram channel, 20 March 2022, https://t.me/hackencyberarmy/108 or https://archive.ph/P3WqP.

[35] KiberBull, Telegram chat, 14 March 2022, https://t.me/c/1549333360/346.

[36] Studentcyberarmy, Telegram channel, 22 March 2022, https://t.me/studentcyberarmy/209 or https://archive.ph/DnK1M.

[37] Anonymous-Ukraine, Telegram channel, 23 March 2022, https://t.me/ciberwars/740 or https://archive.ph/ShKfQ.

asna[.]ru.[38] Notably absent in the entire information exchange was Hacken.io.

Date & Time	Channel or Chat	Target information shared
14-Mar, 09:11	IT Army of Ukraine channel	178.248.235.156
14-Mar, 09:11	IT Army of Ukraine chat	178.248.235.156
22-Mar, 10:38	Studentcyberarmy channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22-Mar, 10:39	CyberFire chat	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22-Mar, 10:39	DDoS Attack Cyber Cossacks Chat	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22-Mar, 10:51	Cyber Cerber channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
22-Mar, 11:35	DDoS Attack Cyber Cossacks channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:08	Cyber Palyanitsa channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:17	Cyber Cerber channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:25	Anonymous Ukraine channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:29	Studentcyberarmy channel	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:29	CyberFire chat	178.248.235.156, 5.188.114.85 5.188.116.168, (80 HTTP / 443 HTTPS)
23-Mar, 12:36	DDoS Attack Cyber Cossacks channel	docker run -it --rm --pull always ghcr.io/porthole-ascend-cinnamon/mhddos_proxy:latest http://www.asna.ru/ -t 1500 --rpc 1000 -p 1000 --http-methods STRESS –debug MHDDoS: python start.py STRESS http://www.asna.ru/ 5 1000 proxy.txt 100 3600 true

External Clustering

The third example is “external clustering”, which is when the targeting information fails to circulate widely and only survives in a small cluster of channels and chats. On 28 February and 3 March, the URL of mvideo[.]ru was mentioned in the disBalancer Ukraine chat and the CyberFire chat. Mvideo is one the largest consumer electronics chains in Russia. The call to target mvideo was not picked up by anyone until two weeks later when Cyber Palyanitsa posted 3 of mvideo’s IPs and 18 different ports at 9.19 p.m. CET. Eleven minutes later the Studentcyberarmy posted the exact same targeting information, and literally within the same minute the post was forwarded in the CyberFire chat. At 10.21 p.m., Cyber Cerber picked up the information as well. On 7 May, the IT Army finally picked up mvideo as a DDoS target with one IP overlapping from the previously shared target information.[39] A group known as Ukrainian Reaper posted the commands to update Multiddos via docker and MHDDoS via Python.[40]

Note: Multiddos is a DDoS script that is exclusively being used by Ukrainian Reaper. It combines three tools: auto_mhddos developed by Ukrainian Reaper, db1000n, and UA Cyber Shield.[41] The latter two will be discussed in the next section.

Date & Time	Channel or Chat	Target information shared
28-Feb, 08:20	disBalancer Ukraine chat	mvideo.ru
3-Mar, 15:53	CyberFire chat	mvideo.ru
19-Mar, 21:19	Cyber Palyanitsa channel	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19-Mar, 21:30	Studentcyberarmy channel	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19-Mar, 21:30	CyberFire chat	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
19-Mar, 22:21	Cyber Cerber channel	185.71.67.88 (80/http, 443/HTTP); 5.188.118.38 (22/SSH, 80/http, 123/NTP, 443/HTTP, 3306/MYSQL, 44060/Unknown); 37.140.192.237 (21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 111/PORTMAP, 143/IMAP, 3306/MYSQL)
7-May, 08:00	IT Army of Ukraine channel	mvideo.ru/tehnika-dylya-kuhni 185.71.67.88 (80/TCP, 44/TCP) api.mvideo.ru webapi.mvideo.ru 185.71.67.88 (80/TCP, 443/TCP)
7-May, 10:29	Ukrainian Reaper	multiddos (Layer 4 + 7) docker run -it --rm --log-driver none --name multidd --pull always karboduck/multidd mhddos_proxy (Layer 4 +7): python3 runner.py --itarmy --http-methods GET STRESS -t 250

Ad Hoc Prioritization

The fourth example is on what might be adequately termed “ad hoc prioritization”. Here, bits and pieces of targeting information pop up now and then in various channels and chats but are only consolidated at a much later point in time when the target is designated high priority by the IT Army. Between February 28 and March 4, the targeting of qiwi[.]com was widely discussed in the IT Army chat, the CyberFire chat, and the two disBalancer chats. QIWI is a popular Russia payment service provider that also serves the other members of the Commonwealth of Independent States (CIS). Multiple users on Telegram asked why QIWI was not being announced as a DDoS target. One user for example quipped that QIWI should not be targeted because there needs to be at least one path to send money from Russia to Ukraine. Others

[38] DDoS Attack Cyber Cossacks, Telegram channel, 23 March 2022, https://t.me/ddos_separ/903 or https://archive.ph/584td.

[39] IT Army of Ukraine, Telegram channel, 7 May 2022, https://t.me/itarmyofukraine2022/331 or https://archive.ph/QkT15.

[40] Ukrainian Reaper, Telegram channel, 7 May 2022, https://t.me/ukrainian_reaper_ddos/244 or https://archive.ph/fYerr.

[41] https://web.archive.org/web/20220608113119/https://github.com/KarboDuck/multiddos/blob/main/README.md. Also see: Ukrainian Reaper, “Ukrainian reaper in touch. DDOS-imo RF using Multiddos,” *Mezha*, 21 May 2022, https://web.archive.org/web/20220608104948/https://mezha.media/articles/ddos-rf-z-multiddos/.

were simply stating that they were now DDoSing QIWI individually.

The dynamics changed on 4 March, when QIWI released a press statement noting that "U.S. and EU sanctions targeting Russia have had no immediate material impact on QIWI's operations. Neither QIWI nor any of its subsidiaries is specifically targeted by the new sanctions enacted as a result of the Russian military operations in Ukraine".[42] On the same day, the "DDoS Attack Cyber Cossacks" channel (around 69,800 subscribers) announced the targeting of QIWI and published one IP and two ports.[43] A few hours later the target was changed to a different QIWI IP in a post explaining, "let's try with more people, start 9:23, attack to the point until I give a new goal".[44] The discussion on targeting QIWI kept on going for the next 25 days, with different channels and chats publishing other QIWI IPs and running their own DDOS attacks. Then on 29 March, the IT Army channel surprisingly announced that "we have a need to attack QIWI now".[45] The post covered 15 QIWI IPs and ports, including all those that were previously circulated in different channels and chats. For whatever reason, on that very day, the IT Army decided to designate QIWI a high priority DDoS target that needed to be taken down immediately.

Notably, ad hoc prioritization was also at play when EGAIS was targeted by the IT Army in early May 2022. EGAIS is the Russian government's unified state automated alcohol accounting information system, which is the centralized systems that certifies and taxes every bottle of alcohol, vodka, and wine produced in Russia. Back in early April 2022, one user in the IT Army's chat brought up EGAIS three times as being a good DDoS target. As the user himself explained on 4 April, "believe me, this goal is quite serious because it causes reputational damage. This portal belongs to the state and shops and distributors must confirm exactly according to the law of the Russian Federation to wait for documents in this portal".[46]
On 2 May at 8.00 a.m., EGAIS was picked up as a target by the DDoS Attack Cyber Cossacks.[47] And at 8.55 a.m. the IT Army channel announced that "today's target was received from one of our subscribers. EGAIS is a Russian federal state-owned automatic system for tracking the production and distribution of alcoholic beverages in the country. If this system is down, the official turnover of liquor and spirits in Russia will be blocked!"[48]

According to Russian media outlet Vedomosti, "producers and distributors of alcohol for the first May holidays could not ship products to their customers due to a large-scale failure in the operation of [EGAIS]."[49] Between 2 May and 12 May, the IT Army designated EGAIS a high priority target. On 7 May for example, the IT Army channel noted that "today, online shopping Russia will be cancelled ;) And don't forget to keep 'EGAIS'".[50] Similarly on 8 May, the channel explained, "we have a tradition to combat Russian propaganda on Sunday. Let's stick to it. Additionally, we'd like to keep a firm grip on 'EGAIS' because due to your help, there is an ongoing flow of complaints about this service".[51]

According to the Russian Foreign Ministry, "as of May 2022, over 65,000 'sofa hackers' from the USA, Turkey, Georgia, and EU countries regularly took part in coordinated DDoS attacks on [Russia's] critical information infrastructure".[52]

IT Army Coordination Document

Now that we have a sense of how the visible sharing of DDoS targeting information works on Telegram, let us take a look at the publicly accessible IT Army coordination document which is hosted on Google Docs and shared by the official IT Army Telegram bot.[53] For this write-up the most recent version was accessed on 30 March.

The coordination document is sporadically being updated by the IT Army and includes information on the priorities of DDoS targets. It also roughly tracks which websites are down or need to be re-engaged, and it serves as a resource to several DDoS tooling instructions as a guide for

[42] QIWI, "QIWI States its Operations Remain Uninterrupted," 4 March 2022, https://web.archive.org/web/20220608113203/https://investor.qiwi.com/news-and-events/press-releases/3994532231/.

[43] DDoS Attack Cyber Cossacks, Telegram channel, 4 March 2022, https://t.me/ddos_separ/482 or https://archive.ph/Sqd3t.

[44] DDoS Attack Cyber Cossacks, Telegram channel, 4 March 2022, https://t.me/ddos_separ/495 or https://archive.ph/i6dtw.

[45] IT Army of Ukraine, Telegram channel, 29 March 2022, https://t.me/itarmyofukraine2022/247 or https://archive.ph/x0cHA.

[46] IT Army of Ukraine, Telegram chat, 4 April 2022.

[47] DDoS Attack Cyber Cossacks, Telegram channel, 2 May 2022, https://t.me/ddos_separ/1186 or https://archive.ph/mecvB.

[48] IT Army of Ukraine, Telegram channel, 2 May 2022, https://t.me/itarmyofukraine2022/321 or https://archive.ph/IR1Gv.

[49] Anna Kiseleva and Margarita Sobol, "У производителей и дистрибуторов алкоголя возникли сложности с поставками продукции," *Vedemosti*, 4 May 2022, https://web.archive.org/web/20220608113248/https://www.vedomosti.ru/business/articles/2022/05/04/920913-u-proizvoditelei-i-distributorov-alkogolya-voznikli-slozhnosti-s-postavkami-produktsii.

[50] IT Army of Ukraine, Telegram channel, 7 May 2022, https://t.me/itarmyofukraine2022/331 or https://archive.ph/QkT15.

[51] IT Army of Ukraine, Telegram channel, 8 May 2022, https://t.me/itarmyofukraine2022/333 or https://archive.ph/BgFxi.

[52] Ministry of Foreign Affairs of the Russian Federartion, "Answer of the Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia A.V. Krutskikh to a media question about attacks on Russian critical infrastructure," 9 June 2022, https://www.mid.ru/ru/foreign_policy/news/1817019/ or https://archive.ph/8U6CN.

[53] IT Army Coordination Document, accessed 30 March 2022, https://docs.google.com/spreadsheets/d/1xDbYcqCteABOZo3gGGP2uHG-0i3f-UuMGbNZ-Bo_W8Q/edit?usp=drivesdk.

newcomers.[54] On the DDoS target prioritization part, the document shows that the IT Army only had two priority designations at the time. Russian online banking services like Sberbank and payment processors such as Mirconnect were designated priority tier one. Online tellers like cse[.]ru were deemed priority tier two. Notably, as of this writing, QIWI was still absent from the priority list, yet it did appear under a separate tab called "find_ip_port", with no IP and ports yet scribbled in, illustrating the ad hoc nature of the IT Army targeting QIWI. Interestingly, the document also had a tab called "IP&Port", which on 30 March only included the URLs, IPs, and ports of six Russian Ministries. Those targets were published by the IT Army channel on 30 March at 1.48 p.m. CET. Apart from these six targets there are no other IPs and ports listed in the entire coordination document.

Overall, the IT Army has been primarily utilizing the coordination document as an introductory guide to newcomers which is why it included two DDoS attack level categories: "attack: simple level" and "attack: advanced level".

The simple level lists four DDoS sites. Users load these websites in their browser, then a script on the website continuously sends requests to a pre-set list of designated targets. Some DDoS websites display which sites they are targeting while others do not. Probably the most popular DDoS attack website listed in the IT Army's coordination document is playforukraine[.]org. The website was developed by members of the Lviv IT cluster and gamifies DDoS attacks by engaging users with the popular numerical puzzle game 2048.[55] Playforukraine stands apart from other DDoS websites for four reasons: (a) it was launched on 28 February, only four days after the Russian invasion started;(b) it claims to be verified by the Ukrainian Cyberpolice; (c) it was promoted on the official Lviv Regional Administration website; and (d) it has been officially endorsed by the Ukrainian Ministry of Digital Transformation and even the Ukrainian Parliament.[56]

Speaking to *FastCompany*, the developers explained that "one user can send 20,000 server requests in one hour of gameplay".[57] On 3 March, playforukraine tweeted that "123k players performed 153 bln attacks".[58] Playforukraine does not reveal which sites it is targeting, but the occasional screenshot posted on their Twitter account shows web check results for dominopizza[.]ru, alfabank[.]ru, and gazprom[.]ru.[59] As with all other attack vectors, playforukraine notes on its website that "before starting the game, turn on the [Virtual Private Network] if you play from the territory of Ukraine".[60] This essentially means that users using VPNs route their traffic through a server located outside Ukraine – most notably EU and NATO member states – to DDoS Russian sites. The reasons for doing this are manifold, with the primary one being that Russia companies have blacklisted Ukrainian IPs.

When it comes to the advanced level DDoS attacks, the IT Army's coordination document is rather outdated, as it includes step-by-step manuals that were drawn up back in late February. These include instructions such as utilizing free trial periods for virtual servers in the cloud – offered by AWS, Google, and Microsoft – to install DDoS attack tools. Other instructions cover a handful of GitHub repositories to set up dockers and "stress testers/DDoS testing tools", including GoldenEye and Slowloris which are pretty old school.[61] GoldenEye's initial releases was back in 2012 and Slowloris three years before that.[62]

A site called ddosukraine[.]com.ua has communicated a clearer understanding of what the IT Army means by advanced level attacks. Initially it was unknown who set-up the site, but in March the official IT Army channel bot started to recommend the site every 15 minutes in the IT Army Telegram chat. The website also linked exclusively to the IT Army channel and refresheed every 15 minutes to show the latest targeting information published by the IT Army.[63]

---

[54] With the create of the official IT Army of Ukraine website (itarmy.com.ua), the coordination document was subsequently discontinued.

[55] Mark Sullivan, "This game crowdsources cyberattacks against Russian websites," *FastCompany*, 18 March 2022, https://web.archive.org/web/20220608145943/https://www.fastcompany.com/90732766/ddos-play-for-ukraine-russian-cyberattack.

[56] PlayforUkraine, Twitter, 28 February 2022, https://web.archive.org/web/20220509133130/https://twitter.com/playforukraine1/status/1498273795366293505; Loda.gov.ua, "Львівські ІТ-спеціалісти створили онлайн гру для допомоги Україні у боротьбі з російською агресією," 28 February 2022, https://web.archive.org/web/20220509121148/https://loda.gov.ua/news?id=65972; Ministry of Digital Transformation, Telegram channel, 15 March 2022, https://t.me/mintsyfra/2763 or https://archive.ph/LHhEe; Ministry of Digital Transformation, Telegram channel, 12 April 2022, https://t.me/mintsyfra/2908 or https://archive.ph/M5LJE; Verkhovna Rada of Ukraine, Telegram channel, 15 March 2022, https://t.me/verkhovnaradaofukraine/1347.

[57] Sullivan, "This game crowdsources cyberattacks against Russian websites."

[58] PlayforUkraine, Twitter, 3 March 2022, https://web.archive.org/web/20220509133153/https://twitter.com/playforukraine1/status/1499425742962184192.

[59] PlayforUkraine, Twitter, 18 March 2022, https://web.archive.org/web/20220509132632/https://twitter.com/playforukraine1/status/1504797556513067013; PlayforUkraine, Twitter, 17 March 2022, https://web.archive.org/web/20220509132848/https://twitter.com/playforukraine1/status/1504487841467826189; PlayforUkraine, Twitter, 5 March 2022, https://web.archive.org/web/20220509132906/https://twitter.com/playforukraine1/status/1500161959911731201.

[60] PlayforUkraine, Website, 9 May 2022, https://web.archive.org/web/20220509133002/https://playforukraine.org/.

[61] GoldenEye, Github, accessed 8 June, https://web.archive.org/web/20220608104809/https://github.com/jseidl/GoldenEye; Slowloris, Github, accessed 8 June, https://web.archive.org/web/20220608095923/https://github.com/gkbrk/slowloris.

[62] Zion3r, "[GoldenEye v2.0] DoS Tool," Kitploit.com, 23 January 2014, https://web.archive.org/web/20220613151215/https://www.kitploit.com/2014/01/goldeneye-v20-dos-tool.html?m=0; RSnake & John Kinsella, "Slowloris HTTP DoS," ha.ckers.org, accessed 8 June, https://web.archive.org/web/20090822001255/http://ha.ckers.org/slowloris/.

[63] DDoSUkraine, Website, 1 April 2022, https://web.archive.org/web/20220401160219/https://ddosukraine.com.ua/.

Under the section on "powerful tools", one set of instructions details how to set up a virtual machine to run "Death by 1000 needles" (db1000n). Db1000n is a GitHub repository authored by Arriven aka. Bohdan Ivashko, a senior software engineer working out of Kyiv for Palo Alto-headquartered US-headquartered computer network security company Cyberhaven.[64] Db1000n is special to the degree that (a) it was uploaded onto GitHub on 26 February in direct response to the Russian invasion, (b) its official manual notes that "this is an instruction manual for those who want to provide their computers to the centralized management of the Ukrainian IT Army", (c) it is mentioned more than 680 times in the IT Army chat, and (d) it serves as a foundation for several git clones that are IT Army inspired.[65]

For example, the instructions for db1000n on the ddosukraine[.]com site linked to a Google Drive folder with a docx file that read: "My name is Igor, I'm an IT specialist from Lviv. At first, I came across a channel in the Telegram 'IT Army of Ukraine'. There I learned that there is a ready-made program 'Death by 1000 needles', created to bring down the sites of Mordor, as well as that it needs to run via VPN. Working for a week, I assembled a virtual shell machine for Death by 1000 needles. My shell turned out to be quite successful, so I decided to share it with others".[66]

In early April, the ddosukraine[.]com.ua site moved to the new domain itarmy[.]com.ua. The official IT Army bot has been promoting the site ever since, and the IT Army channel has endorsed it as the official IT Army of Ukraine website. Probably the most intriguing change that was introduced on the new site was an announcement on 5 April that stated "very important! For an effective attack, we must all strike at the same targets and keep them in that position for as long as necessary. Therefore, we ask you not to join in the chats and not to launch independent attacks on other targets".[67]

GitHub Repositories

As of this writing, the number one GitHub repository discussed in the IT Army chat – with around 1070 mentions – is called MHDDoS. MHDDoS is not in any way affiliated with the IT Army and its author explicitly notes in the repository's readme, "Please Don't Attack websites without the owner's consent".[68] The most shared MHDDoS clone in the IT Army chat is called MHDDoS_proxy authored by a user named porthole-ascend-cinnamon.[69] In the GitHub repository readme file, porthole-ascend-cinnamon links to an unofficially guide called "DDoS-for-all", authored by a user named SlavaUkraineSince1991.[70] It did not come as a surprise that the examples SlavaUkraineSince1991 used in his guide were ria[.]ru and tass[.]ru. What did come as a surprise was that the guide linked to three different Telegram channels with none of them being the IT Army: "DDOS Tutorial for all" (around 5,800 subscribers), "KiberBull" (around 7,700 subscribers), and "Ukrainian Reaper" (around 4,800 subscribers).[71]

Looking at the three channels in question, a few things stick out. All three occasionally pick up targets that are announced by the IT Army channel. KiberBull for example, was the only channel visible to me that re-posted the target information for asna[.]ru on 14 March. By contrast, Ukrainian Reaper officially stated on 1 March that they are sourcing their targets from the IT Army channel and a Telegram channel called "ddoskotyky" (around 20,100 subscribers).[72] In some instances, DDOS Tutorial for all and Kiberbull decided to help the IT Army finish off their targets, as was the case on 19 March when the IT Army announced the targeting of Tutu[.]ru, Russia's largest rail and flight ticket booking service. DDOS Tutorial for all explained that "we help IT Army of Ukraine to finish tutu[.]ru", and KiberBull equally posted that "we will help IT-Army to put [out] one of the largest ticket booking services [tuttu[.]ru]".[73] Overall, however, these three channels do not seem to act as one coherent group, except for

[64] Db1000n, ReadMe.md, Github, 8 June 2022, https://web.archive.org/web/20220608094714/https://github.com/Arriven/db1000n; Arriven, Github, 8 June 2022, https://web.archive.org/web/20220608094644/https://github.com/arriven; Cyberhaven, "Our Mission," accessed 8 June, https://www.cyberhaven.com/about-us/.

[65] Db1000n, Releases, Github, 8 June 2022, https://web.archive.org/web/20220608094937/https://github.com/Arriven/db1000n/releases?page=9; Death by 1000 needles, 24 March 2022, https://web.archive.org/web/20220324210843/https://telegra.ph/death-by-1000-needles-03-18; Db1000n Hotspotshield, Github, 8 June 2022, https://web.archive.org/web/20220608095015/https://github.com/gidiyan/db1000n_hotspotshield.

[66] Google translate of: https://docs.google.com/document/d/1puI2_V5_oyc-1cA4a3yuwl8J2_O4ooybOHuU1fR261k/edit. Document title unknown, accessed in March 2022.

[67] IT Army of Ukraine, Website, 5 April 2022, https://web.archive.org/web/20220405192723/https://itarmy.com.ua/.

[68] MatrixTM, MHDDoS, Readme.md, Github, 8 June 2022, https://web.archive.org/web/20220608095847/https://github.com/MatrixTM/MHDDoS/blob/main/README.md.

[69] Porthole-ascend-cinnamon, MHDDoS_proxy, Readme.md, Github, 8 June 2022, https://web.archive.org/web/20220608105000/https://github.com/porthole-ascend-cinnamon/mhddos_proxy.

[70] SlavaUkraineSince1991, DDoS-for-all, MHDDoS_proxy.md, Github, 8 June 2022, https://web.archive.org/web/20220608104915/https://github.com/SlavaUkraineSince1991/DDoS-for-all/blob/main/MHDDoS_proxy.md.

[71] Note: Ukrainian Reaper was likely included in the list because their multiddos tool is partially build upon MHDDoS_proxy. See: Ukrainian Reaper, "Український жнець на зв'язку. DDOS-имо РФ за допомогою Multiddos," *Mezha*, 21 May 2022, https://web.archive.org/web/20220608104948/https://mezha.media/articles/ddos-rf-z-multiddos/.

[72] Ukrainian Reaper, Telegram channel, 1 March 2022, https://t.me/ukrainian_reaper_ddos/5 or https://archive.ph/5W3Jo.

[73] DDoS Tutorial for All, Telegram channel, 19 March 2022, https://t.me/ddos_for_all/103 or https://archive.ph/Io3lq.

one oddity: DDOS Tutorial for all does occasionally support KiberBull and Ukrainian Reaper in their individual DDoS campaigns that are not IT Army designated targets.[74]

Should these three groups be considered part of the IT Army? Yes and no. On the one hand, they do occasionally participate in the IT Army's DDoS campaigns. On the other hand, the IT Army itself explained in a Telegram post on 4 April: "there are quite a few channels that conduct DDoS attacks on hostile services with us. Each community has a database of tutorials, as well as a sufficient number of involved participants. It is important to understand that each community is independent and chooses priority goals for itself. But we all communicate with each other and quite often they support us in attacks on our targets. We want to thank our subscribers and the following communities for their active position and help in the fight against the enemy in cyberspace".[75] Among the communities listed are Ukrainian Reaper and KiberBull, but also Cyber Palyanitsa, Studentcybergroup, DDoS Attack Cyber Cossacks, Anonymous-Ukraine, DDoS joint group, and UA Cyber Shield – which we are going to look at next.

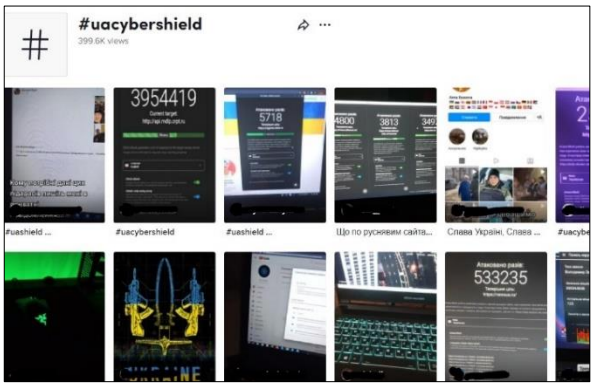
Sidenote: Cyber Palyanitsa echoes the IT Army's sentiment. On its website it lists several coordinating groups stating "Choose your legion. Each of our groups has both common and individual tasks, join and help Ukraine with us!"[76]

Source: cyberarmy[.]com.ua

The third GitHub repository that has been popping-up in various Telegram channels is called UA Cyber Shield or uashield for short. Uashield is a DDoS tool that was uploaded onto GitHub on 28 February. It is a project by a group that calls itself the "Volunteer cyber defense of Ukraine". Uashield stands out because of four oddities: (a) on the group's website - help-ukraine-win.super[.]site – they display an official Ukrainian government logo with the note, "supported by the Cabinet of Ministers of Ukraine"; (b) in its GitHub readme they explain that "ALERT!!! We are not supporting unlawful active attacks or malware campaigns that are causing technical harms. Use only for educational purposes. You can only try this platform on your own website!"; (c) they are the only DDoS tool I am aware of whose instructions have been translated into 11 different languages, including Korean and Portuguese; and (d) on 31 March, the official uashield Telegram channel stated that "starting from the current version UA Cyber SHIELD supports all attack types used by the IT Army of Ukraine: HTTP / HTTPS / UDP".[77] Four days later, uashield officially announced that "we are working together with the IT ARMY of Ukraine".[78]

Source: help-ukraine-win.super[.]site

Notably, with uashield running on almost all operating systems – including mobile OS – combined with its prominent attack counter user interface, it has almost naturally attracted the attention of many young non-technical users who in turn have posted several videos of their own uashield use on TikTok.[79]



Source: TikTok.com search for "uacybershield"

[74] DDoS Tutorial for All, Telegram channel, 21 March 2022, https://t.me/ddos_for_all/110 or https://archive.ph/xFH98; DDoS Tutorial for All, Telegram channel, 19 March 2022, https://t.me/ddos_for_all/102 or https://archive.ph/bamMR.

[75] IT Army of Ukraine, Telegram channel, 4 April 2022, https://t.me/itarmyofukraine2022/265 or https://archive.ph/ANHcd.

[76] Cyber Palyanitsa, Website, accessed 17 June 2022, https://web.archive.org/web/20220617064032/https://cyberarmy.com.ua/

[77] UA Cyber Shield, "Help Ukraine Win," n.d., https://web.archive.org/web/20220509131644/https://help-ukraine-win.super.site/; Opengs, uashield, readme-en.md, Github, 8 June 2022, https://web.archive.org/web/20220608105100/https://github.com/opengs/uashield/blob/master/README-en.md; UA Cyber Shield, "KR - Help Ukraine," accessed on 9 May, https://web.archive.org/web/20220509131841/https://help-ukraine-win.super.site/kr-help-ukraine; UA Cyber Shield, Telegram channel, 31 March 2022, https://t.me/uashield/22 or https://archive.ph/QKlqY.

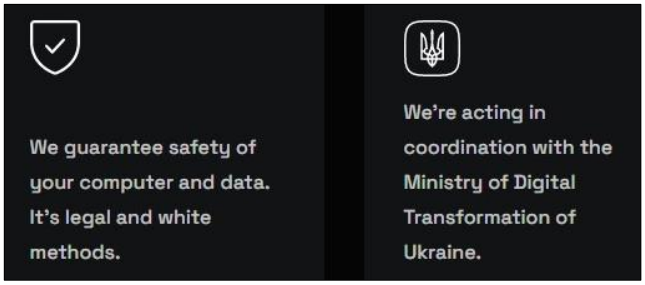
[78] UA Cyber Shield, Telegram channel, 4 April 2022, https://t.me/uashield/33 or https://archive.ph/dfGOf.

[79] Tiktok search for "uashield" and "uacybershield," https://www.tiktok.com/tag/uashield; https://www.tiktok.com/tag/uacybershield.

The fourth GitHub repo is called disBalancer. DisBalancer was designed by a team of cybersecurity and cryptocurrency enthusiasts and was launched under the umbrella of the Hacken Foundation on 2 March 2021. It markets itself as a web3 decentralized DDoS protection network. Essentially, users anywhere can install disBalancer and become members (or farmers as they are called) in a de-centralized network by renting out unused bandwidth and storage space. In return they are rewarded with DDoS tokens that can be bought and sold on most cryptocurrency exchange platforms. As disBalancer explains it: "It works similarly to a blockchain mining pool by setting up a computer node to perform the required operations and receive traffic".[80] Businesses that are interested in implementing disBalancer as a DDoS protection solution simply have to add their network nodes to the DNS records and "all traffic starts circulating behind the nearest ones available. Each node can then redirect traffic to others nearby to increase capacity as required".[81] At its core, disBalancer was inherently conceptualized as a defensive tool to offload incoming DDoS traffic. As the team itself explains, "we strive to defend companies with servers and services on the Internet against DDoS attacks. Our network will act as a warrantor, sharing unused computer power and bandwidth with companies that need these resources. Thereby we will make the world a safer place and change the meaning of DDoS to the good side".[82] So far so good.

4 Hacken, Liberator, and Hackenproof

The problem for Estonia-headquartered Hacken.io started on 4 March when the disBalancer team launched a DDoS attack tool called the Liberator. Liberator was developed in reaction to the Russian invasion with the overarching goal of "helping liberate Ukraine" by DDoSing "Russian propaganda websites and sources that contribute to the Russian invasion of Ukraine".[83] The disbalancer team essentially switched from DDoS defense to DDoS offense by explaining, "don't ask us how legal DDoS attacks on Russian propaganda sites are. Our cities are bombarded where children and civilians die. We are acting in coordination with the Ministry of Digital Transformation that initiated the Ukrainian Cyber Army invention [IT Army] to help the Armed Forces of Ukraine".[84] By tapping into the community disBalancer had built over the past year, users across the globe who previously ran the disBalancer DDoS protection tool now heeded the call and installed Liberator for offensive purposes. For good measure, disBalancer also reminded their followers that, "if you think that this does not concern you or disagree with our participation in fighting against Russian aggression, just leave us forever. Indifference is no less a crime when it comes to other people's lives".[85] As of this writing, disBalancer claims that Liberator was downloaded 100,000+ times, and between 3,000-6,000 users are running the application at any given point in time. If this were not enough to convince people to participate, the disBalancer website notes that (a) "we guarantee [the] safety of your computer and data. It's legal and white methods" and that (b) "by buying DDOS tokens, anybody can help us to scale the app infrastructure and purchase more servers".[86] This means that the DDoS tokens that users could farm by being part of disBalancer's de-centralized DDoS protection network are now being used as a financial resource to build out Liberator's DDoS attack infrastructure. If by this point users were still unsure whether installing Liberator was a good idea, the disBalancer website reassured them under the Ukrainian coat of arms that "we're acting in coordination with the Ministry of Digital Transformation of Ukraine".[87]



Source: disbalancer.com

So how tightly is disBalancer interwoven with Hacken and the Ministry of Digital Transformation? Well, the disBalancer team leaders are prominently displayed on their website. They include Serhii Dovhopolyi, who works as tech lead and is also on Hacken's Kyiv-based R&D team.[88]

[80] disBalancer, "Introducing disBalancer: Decentralized DDoS Protection," Medium, 2 March 2021, https://web.archive.org/web/20220509130352/https://disbalancer.medium.com/introducing-disbalancer-decentralized-ddos-protection-b5fdb8fcf37f.

[81] Ibid.

[82] disBalancer, "Who we are," disbalancer.com, n.d., https://web.archive.org/web/20220509125532/https://disbalancer.com/about/.

[83] disBalancer, "disBalancer Launches Liberator," *Medium*, 4 March 2022, https://web.archive.org/web/20220509125831/https://disbalancer.medium.com/disbalancer-launches-liberator-a6c145cb88e4.

[84] disBalancer, "disBalancer Stays With Ukraine," *Medium*, 1 March 2022, https://web.archive.org/web/20220509130008/https://disbalancer.medium.com/disbalancer-stays-with-ukraine-689327e0edf6.

[85] Ibid.

[86] disBalancer, Website, accessed on 10 May, https://web.archive.org/web/20220510123739/https://disbalancer.com/.

[87] Ibid.

[88] Serhii Dovhopolyi, Linkedin, accessed on 8 June, https://www.linkedin.com/in/sdovhopolyi/?originalSubdomain=ua.

Oleksandr Horlan is operations lead, and he also works for for Hacken in Kyiv as a penetration tester and security analyst.[89] Dyma Budorin serves as advisor and is also the Co-founder and CEO of Hacken.[90] Finally, Denis Ivanov is an advisor and also the Head of the Expert Group at the Ministry of Digital Transformation.[91] The disBalancer website's privacy notice similarly explains that "we are Hacken OÜ, located at Kai tn 1-5M, Tallinn city, Harju county, 10111, Estonia".[92] This is the physical address of Hacken's headquarter in Estonia, a NATO and EU member state.

Interestingly, on 10 March, *Politico* reported that some 50 employees of Hacken's Kyiv office were relocated to Spain, another NATO/EU member state, for security reasons.[93] Eighteen days later, the IT Army channel officially promoted disBalancer's Liberator to its then-306,000 subscribers for the first time.[94]

On 20 April, disBalancer went on to publish its first recruitment video on Youtube. The video's message stated: "instruction is clear even for a little baby. The most effective DDoS-App against Russian Aggressor. […] Run attacks 24/7 wherever you are. We are the Cyber Army. Join Ukrainian Cyber Army in the first cyber world war. You can become a legend".[95] Eight days later, a US-based Youtube cryptocurrency influencer by the name of Boxmining published an 8-minute-long video urging his 268,000 subscribers to install Liberator to DDoS Russian sites.[96] Boxmining is not just a random Youtube influencer. He visited Hacken's Kyiv office in 2020, and in 2021 he interviewed Hacken's CEO Dyma Burodin on his Youtube channel. Naturally, the video was warmly embraced by disBalancer and the Hacken Forces Telegram channel, as well as on Hacken's Twitter account, which tweeted "how to defend Ukraine with ONE app? Run @thedisbalancer's Liberator! @boxmining, a famous crypto influencer and Hacken's friend, dropped a new video on his Youtube channel with an easy explanation".[97]

Neither Hacken nor Boxmining informed their (mostly young) userbase about the potential legal consequences and blowback from running DDoS and interfering in an international armed conflict. In the US, DDoS attacks may be considered a federal crime under the Computer Fraud and Abuse Act.[98] And in Estonia – where Hacken's headquarter is physically located – DDoS attacks may fulfill the category of computer sabotage, which is punishable by up to 3 years in prison.[99] Notably, back in early April 2022, Russia's FSB detained a system administrator working for a local company in Yalta, Crimea, who installed a DDoS tool on his work computer to run attacks against Russian websites between 24 February and 10 March.[100] He is currently facing five years in prison. It is unknown which exact DDoS tool he used. What we do know is that in mid-May, *The Wall Street Journal* reported that disBalancer/Hacken's Kyiv team moved from Barcelona, Spain, to Lisbon, Portugal, another NATO and EU member state.[101]

Underlining this nonchalance, disBalancer decided to publish three Liberator user interviews on 27 May 2022.[102] It is unknown whether these interviews were conducted with real users or are fictional creations the disBalancer team invented to advertise the use of Liberator. Jase Mo from the US explained that "I started off on the hackenproof.com page and went from there. I found Liberator to be, 'EASY AF' to use. […] Not only has Liberator made it easy AF to join the fight, but has allowed the average person to be a part of the Team that is pulling off the largest most effective DDoS champagne the world has ever seen. I love this shit".[103] Meanwhile, Casimir from Germany stressed the financial side of things: "what

---

[89] Oleksandr Horlan, Linkedin, accessed on 8 June, https://www.linkedin.com/in/o-horlan/?originalSubdomain=ua.

[90] Dyma Budorin, Linkedin, accessed on 8 June., https://www.linkedin.com/in/dyma-budorin-acca-56a98035/?originalSubdomain=ua.

[91] Denis Ivanov, Linkedin, accessed on 8 June, https://www.linkedin.com/in/daivanov/?originalSubdomain=ua.

[92] disBalancer, "Privacy Notice 'DisBalancer,'" disBalancer, 16 February 2022, https://disbalancer.com/legal/PrivacyNotice.pdf.

[93] Laurens Cerulus, "Kyiv's hackers seize their wartime moment," *Politico*, 10 March 2022, https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/ or https://archive.ph/qdyD5.

[94] IT Army of Ukraine, Telegram channel, 28 March 2022, https://t.me/itarmyofukraine2022/245 or https://archive.ph/JobpV.

[95] disBalancer, "Join disBalancer to fight russian propaganda," Youtube, 19 April 2022, https://www.youtube.com/watch?v=iCPwat9G6kA.

[96] Boxming, "I NEED YOUR HELP! How YOU can support Ukraine with ONE app (DISBALANCER)," Youtube, 28 April 2022, https://youtu.be/k9LwqbowGMk.

[97] disBalancer, Telegram channel, 28 April 2022, https://t.me/disbalancer_official/427 or https://archive.ph/94aPY; Hacker Forces, Telegram channel, 28 April 2022, https://t.me/hackencyberarmy/240 or https://archive.ph/nVu3l; Hacken, Twitter, 28 April 2022, https://web.archive.org/web/20220509135045/https://twitter.com/hackenclub/status/1519728201941012481.

[98] Congressional Research Service, "Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress," 21 September 2020, https://sgp.fas.org/crs/misc/R46536.pdf, p. 14; Thomas Reuters Practical Law, "Distributed Denial-of-Service (DDoS) Attack," accessed 8 June, https://web.archive.org/web/20220615115331/https://ca.practicallaw.thomsonreuters.com/7-516-9293?transitionType=Default&contextData=(sc.Default)&firstPage=true.

Shawn Tuma, "Yes, Case Law Says It Really Is A CFAA Violation To DDoS A Website," shawnetuma.com, 9 October 2013, https://web.archive.org/web/20220615113618/https://shawnetuma.com/2013/10/09/yes-case-law-says-it-really-is-a-cfaa-violation-to-ddos-a-website/.

[99] Riigi Teataja, "Estonian Penal Code: §207(1) - Hindering of functioning of computer systems," riigiteataja.ee, 1 January 2015, https://www.riigiteataja.ee/en/eli/522012015002/consolide.

[100] Positive Technologies, "ФСБ задержало жителя Ялты за кибератаки на российские информационные ресурсы," *SecurityLab*, 9 April 2022, https://www.securitylab.ru/news/531066.php or https://archive.ph/paTDo.

[101] David Uberti, "They Fled Ukraine to Keep Their Cyber Startup Alive. Now, They're Hacking Back," *The Wall Street Journal*, 12 May 2022, https://www.wsj.com/articles/they-fled-ukraine-to-keep-their-cyber-startup-alive-now-theyre-hacking-back-11652347802.

[102] disBalancer, "disBalancers Shared Their Cyber Fight Stories," *disBalancer*, 27 May 2022, https://web.archive.org/web/20220529121248/https://blog.disbalancer.com/disbalancers-shared-their-cyber-fight-stories/.

[103] Ibid.

would motivate me even more? Maybe a special kind of disBalancer NFT for the verified users of Liberator. ;) I saw that there might be DDOS NFTs for those who hold more than 1000 DDOS [tokens] until the war is over (which is easy for me because I'm buying more as soon as I can)… But maybe you could make special edition NFTs for the cyber warriors?"[104] And Daniil from Ukraine stressed what else can be done: "Besides being involved in disBalancer, I actively support Ukraine in other ways. For instance, by donating to the Armed Forces of Ukraine and assisting the cyber fight on the side of Ukrainians with other DDoS tools designed to shoot russians down. I use a few other applications like UA Cyber SHIELD, dn1000n, dripper, MHDDos, and 5 sites for DDoS attacks. Besides, I report on russian propaganda telegram groups in order to hinder the lies that spread among the people, including in the occupied territories".[105]

On 8 June 2022, disBalancer announced that Roskomnadzor – Russia's Federal Service for the Supervision of Communications, Information Technology and Mass Media – blocked access to disbalancer[.]com.[106] According to the disBalancer blog the "access restrictions to our site to russian providers and Internet users from russia will not stop our DDoS attacks on russian propaganda websites, government, and infrastructure systems that provide the basis for everyday life and enable the flow of goods, information, and services. Until russia withdraws the last soldier from Ukraine and the ongoing shelling by russian forces stops, we are going to further enhance our activities".[107]

The cooperation between Hacken and the Ukrainian government does not stop there. HackenProof, which is Hacken's bug bounty platform, has been running two vulnerability reporting programs in response to the ongoing war in Ukraine: a defensive and an offensive one. The defensive program was established around 1 March and runs under the name "Call for Ukrainian cyber defense. Stop the war".[108] It is geared toward finding "critical vulnerabilities" in Ukrainian government and infrastructure websites, which HackenProof then reports to the corresponding authorities. As the site explains, "we're looking for vulnerabilities such as RCE, SQLI, RFI/LFI, or data leaks. Please don't waste time on low-/medium-severity vulnerabilities. Save our time for what matters".[109] As of 25 May the program received 291 submissions by 27 authors.[110] According to the Wayback Machine, on 8 March the number stood at 271 submissions by 23 authors.[111] Thus, over the past 2.5 months the program added a mere 20 new submissions.

While the program does not pay any bounties, it is important to understand that for a long-time ethical hackers "could face fines of up to $42,000 USD or even three years in prison for trying to detect bugs in the computer systems of the Ukrainian parliament, ministries, or state companies".[112] Only on 21 April, roughly seven weeks after HackenProof initiated its defensive bug bounty program, did the Ukrainian Parliament adopt the law on "Amendments to the Criminal Code of Ukraine to Increase the Effectiveness of the Fight against Cybercrime in the Conditions of Martial Law", which tweaked the criminal code to enable bug bounty programs for the public sector.[113] As of this writing it is still unclear whether HackenProof's bug bounty program ever ran afoul of Ukrainian law or whether Hacken's physical location in Estonia shielded it from prosecution. It is also unknown whether the program was supported by members in the Ukrainian government, or how exactly HackenProof streamlined its information flow to contact the multitude of Ukrainian authorities and companies affected.

HackenProof's offensive program was started on 27 February and runs under the name "Call for exploits. Stop the war".[114] Similar to the defensive one, HackenProof is only looking for submissions of critical vulnerabilities, including data leaks, which are then "put in the good hands of Ukrainian cyber forces".[115] The focus areas are Russian hosting providers, ISPs, aerospace/air control, SCADA systems, banks, public services, energy/oil/gas, transporta-

---

[104] Ibid.

[105] Ibid.

[106] disBalancer, "Roskomnadzor Has Blocked Access To disBalancer Website," *disBalancer*, 8 June 2022, https://blog.disbalancer.com/roskomnadzor-has-blocked-access-to-disbalancer-website/.

[107] Ibid.

[108] HackenProof, "Call for Ukrainian cyber defense. Stop the war," 8 March 2022, https://web.archive.org/web/20220308143814/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

[109] Ibid.

[110] HackenProof, "Call for Ukrainian cyber defense. Stop the war," 25 May 2022, https://web.archive.org/web/20220525133418/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

[111] HackenProof, "Call for Ukrainian cyber defense. Stop the war," 8 March 2022, https://web.archive.org/web/20220308143814/https://hackenproof.com/ukraine-will-win/call-for-ukrainian-cyber-defense-stop-the-war.

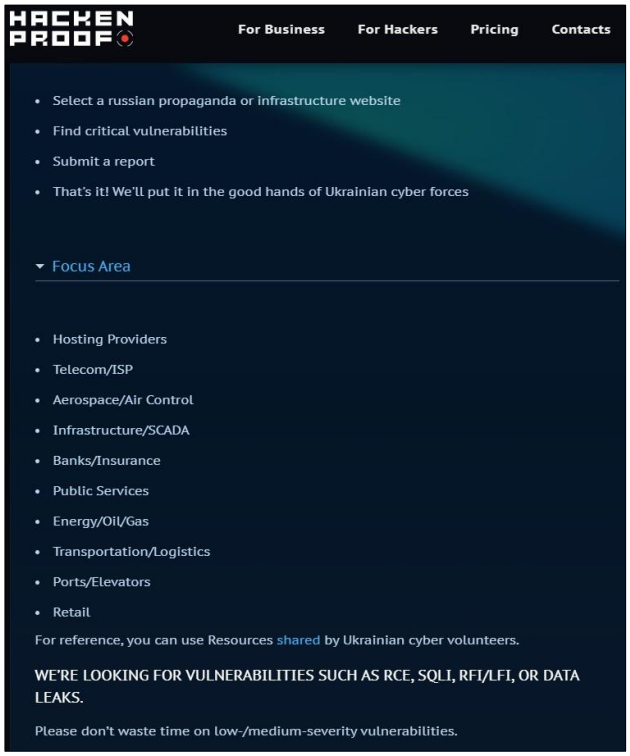
[112] Daryna Antoniuk, "Ukraine reconsiders bug bounties after latest cyberattacks. But are they enough?" *The Record*, 3 February 2022, https://web.archive.org/web/20220608150708/https://therecord.media/ukraine-reconsiders-bug-bounties-after-latest-cyberattacks-but-are-they-enough/.

[113] Ukrinform, "Рада посилила спроможності національної системи кібербезпеки," 24 March 2022, https://web.archive.org/web/20220608150618/https://www.ukrinform.ua/rubric-technology/3438840-rada-posilila-spromoznosti-nacionalnoi-sistemi-kiber-bezpeki.html.

[114] HackenProof, "Call for exploits. Stop the war," 27 February 2020, https://web.archive.org/web/20220227105814/https://hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia.

[115] Ibid.

tion/logistics, ports/elevators, and even retail. It is unclear whether submissions pertaining to the Russian healthcare sector, humanitarian NGOs, schools and universities are also being accepted by HackenProof. Notably, the program site directly links to the IT Army's Telegram channel explaining, "for reference, you can use Resources shared by Ukrainian cyber volunteers".[116] As of 25 May, the program had 422 submissions by 32 authors.[117] According to the Wayback Machine that number has stayed the same since 14 March.[118] Thus, over the past eleven weeks the offensive program received no new submissions. Like the defensive program, there are no bounty pay-outs.



Source: hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia

Surprisingly, the existence of the offensive bug bounty program combined with the fact that it is organized by a company headquartered in Estonia has to date not spurred any legal, ethical, nor political conversations on co-belligerency in cyberspace, the role of Ukrainian-owned companies operating from NATO/EU member states, and their targeting of Russian civilian infrastructure in cooperation with the Ukrainian government. There is also no conversation in the information security community on the role of bug bounty programs targeting a belligerent party embroiled in an international conflict. The current silence on these issues amidst the ongoing war in Ukraine is certainly understandable – and so is the activism of Ukrainians abroad – yet NATO/EU member states might be setting unintended legal and ethical precedents that may create significant political blowback in the future. For example, what if a Russian-owned company located in Germany were to organize an offensive bug bounty program that targets Ukrainian critical infrastructure and shares the discovered vulnerabilities with the Russian intelligence community? Would Berlin, Brussels, and Washington deem this acceptable private sector behavior?

Apart from HackenProof's two bug bounty programs, Yegor Aushev also started his own bug bounty program called "Hack/Fuck Russia" that ran its first phase from 1 March to 10 March. It was financially supported by Aushev's Kyiv-based Cyber Unit Tech company with a donation of 100,000 USD.[119] Curiously, the bug bounty announcement also included a Tether wallet address for donations. To date that wallet has received a combined 70 Tether, which is a mere 70 USD (Tether is pegged 1:1 to USD).[120] Yet, in an interview with *The Record*, a Cyber Unit Tech representative explained that "our company has contributed the initial $100,000, but we see participation and contribution from all over the world. The amounts are very, very significant and might be one of the biggest bounties ever, maybe the biggest 'unofficial' bounty".[121]

So, how do we square these two different assessments? If there is a huge donation flow that underpins Aushev's bug bounty program, then it is certainly not going into the Tether wallet. We also know that neither Aushev nor Cyber Unit Tech have posted any other wallet addresses on their official Twitter, LinkedIn, and Facebook accounts. So, how do people from across the world know to which wallets to donate in support of the cause? One feasible explanation could be that the wallet addresses are spread within invite-only groups on WhatsApp and Signal to facilitate donations from the Ukrainian IT community living abroad. Another possibility might be that the international cryptocurrency donations flowing into the Ukrainian government's official Bitcoin, Thether, and Etherium wallets are partially underpinning Aushev's bug bounty

[116] Ibid.

[117] HackenProof, "Call for exploits. Stop the war," 25 May 2022, https://web.archive.org/web/20220525132844/https://hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia.

[118] HackenProof, "Call for exploits. Stop the war," 14 March 2022, https://web.archive.org/web/20220314082410/https://hackenproof.com/ukraine-will-win/save-millions-lives-hackers-against-russia.

[119] Yegor Aushev, Twitter, 27 February 2022, https://web.archive.org/web/20220509135052/https://twitter.com/Yegor_au/status/1497880962990059522.

[120] Tokenview, "Tether Explorer: THTCwoLQ4dg5uzLLPyaUSbB1x8rYKFAPA3," accessed June 8, https://usdt.tokenview.com/en/address/THTCwoLQ4dg5uzLLPyaUSbB1x8rYKFAPA3.

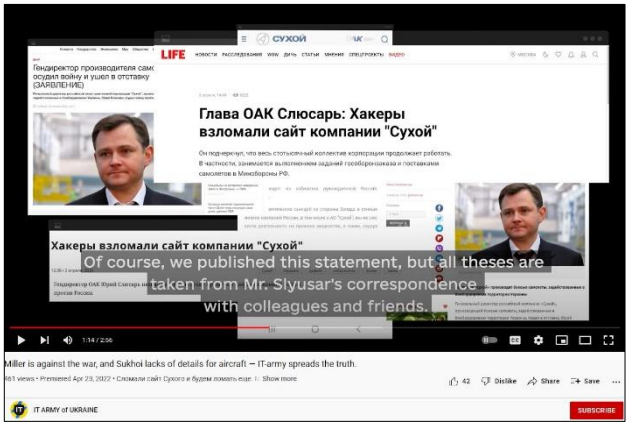
[121] Adam Janofsky, "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites," *The Record*, 4 March 2022, https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/ or https://archive.ph/38X95.

program.[122] As of 21 April, neither Aushev nor Cyber Unit Tech has announced the start of phase two of their bug bounty program. It is unknown whether the program actually paid out any bounties or to whom any of the reported vulnerabilities were forwarded. Given Aushev's closeness to the Ukrainian government and Cyber Unit Tech's strategic partners – which includes the National Security and Defense Council of Ukraine – we can infer with some level of confidence that the vulnerabilities might have ended up in the hands of the Ukrainian Ministry of Defense, the intelligence services, or the IT Army.

5 Non-public Structure and Tasks

Apart from the publicly visible IT Army structures and tasking flows, there also exists an in-house section to the IT Army.

Hints of the in-house section first popped up in early March when the IT Army defaced miranda-media[.]ru, which is a Russian ISP serving the Crimean Peninsula.[123] Several other defacements followed of which almost none gained widespread media attention. The exception occurred on 2 April and 6 April, when the websites of Sukhoi[.]ru and Gazprom[.]ru were defaced with fake statements by Yuri Slyusar (General Director of Sukhoi) and Alexie Miller (CEO of Gazprom) criticizing the Kremlin for the war in Ukraine.[124] At the time, public speculations veered between the websites being hacked by an unknown group and the statements being legitimate. The fog of war was lifted three weeks later on 23 April, when the IT Army's channel posted a three-minute video in which it took credit for the fake statements. As the video explains, "we published the statement, but all [the content was] taken from Mr. Slyusar's correspondence with colleagues and friends. […] Within the Kremlin's inner circle people know about [Alexie Miller's] position for a long time. We just made it public, completely collecting his thoughts from the correspondence".[125] As of this writing, discussions pertaining to defacements are entirely absent from both the IT Army channel and chat.



Screenshot of the IT Army video posted on April 23, 2022, in the IT Army's Youtube channel

On 4 April, the IT Army posted a two-minute video on the use of Clearview in Ukraine to identify Russian soldiers.[126] Clearview is a controversial US-headquartered AI facial recognition company that has assembled a vast biometric database – by scraping facial pictures from social media and the wider Internet – to readily identify and locate any individual. The company is currently facing several lawsuits in the US and has been fined by various privacy watchdogs in the EU.[127] On 23 May, the UK's Information Commisioner's Office fined Clearview more than 7.5 million GBP and ordered the company to delete all the data of UK residents from its systems.[128] Kashmir Hill at *The New York Times* explained Clearview's impact best by stating that, "searching someone by face could become as easy as Googling a name. Strangers would be able to listen in on sensitive conversations, take photos of the participants and know personal secrets. Someone walking down

[122] Kevin Reynolds, "Ukrainian Government Receives Nearly $10M in Crypto Donations After Russian Invasion," *CoinDesk*, 26 February 2022, https://www.coindesk.com/business/2022/02/26/ukrainian-government-is-seeking-crypto-donations/ or https://archive.ph/q5Yn3; Christopher Robbins, "The Growing Digital Asset Lifeline in Ukraine," *CoinDesk*, 31 March 2022, https://www.coindesk.com/markets/2022/03/31/the-growing-digital-asset-lifeline-in-ukraine/ or https://archive.ph/0pYX0.

[123] Stefan Soesanto, Twitter, 12 March 2022, https://web.archive.org/web/20220608105346/https://twitter.com/iiyonite/status/1502658550937567232, Video shows the defaced website at timestamp: 0:15; https://www.youtube.com/watch?v=o4Wi5rFemro.

[124] Stefan Soesanto, Twitter, 24 April 2022, https://web.archive.org/web/20220608105316/https://twitter.com/iiyonite/status/1518189001819279360; "Website of Russian oil firm Gazprom Neft goes down after apparent hack," *Reuters*, 6 April 2022, http://web.archive.org/web/20220608151249/https://www.reuters.com/business/energy/russian-oil-company-gazprom-nefts-website-appears-have-been-hacked-2022-04-06/; Olexander Scherba, Twitter, 2 April 2022, https://twitter.com/olex_scherba/status/1510185641547640832 or https://archive.ph/FCYL2.

[125] IT Army of Ukraine, Telegram channel, 23 April 2022, https://t.me/itarmyofukraine2022/310 or https://archive.ph/c1UBk.

[126] IT Army of Ukraine, "IT-army of Ukraine: an appeal to Russians," Youtube, 4 April 2022, https://youtu.be/AYJSBSmLlnU; IT Army of Ukraine, Telegram channel, 4 April 2022, https://t.me/itarmyofukraine2022/267 or https://archive.ph/e7eCI.

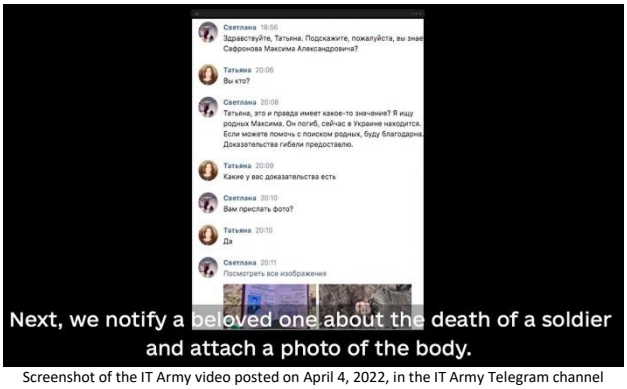
[127] Adam Schwartz, "Victory! More Lawsuits Proceed Against Clearview's Face Surveillance," *Electronic Frontier Foundation*, 15 February 2022, http://web.archive.org/web/20220608151243/https://www.eff.org/deeplinks/2022/02/victory-another-lawsuit-proceeds-against-clearviews-face-surveillance; Privacy International, "Challenge against Clearview AI in Europe," accessed June 8, http://web.archive.org/web/20220608151333/https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe.

[128] ICO, "ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted," *ICO*, 23 May 2022, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

the street would be immediately identifiable — and his or her home address would be only a few clicks away. It would herald the end of public anonymity".[129]

On 13 March, *Reuters* reported that the Ukrainian Defense Ministry started to use Clearview to identify dead Russian soldiers.[130] Ten days later, Ukraine's Minister of Digital Transformation, Mykhailo Federov, explained on Telegram that "today, we use artificial intelligence to search the social media accounts of dead Russian soldiers for photos of corpses, to report their deaths to friends and relatives, to dispel the myth of a 'special operation' in which 'no conscripts' and 'no one dies.'"[131] Exact figures on Clearview's use in Ukraine were hard to come by until the IT Army posted its video on 4 April. In it, the IT Army explained that it uses Clearview to directly contact dead soldiers' families and loved ones via social media and messaging apps, by informing them about the death of their relative and attaching a picture of the mutilated corpse and passport. While many Western outlets went on to described Ukraine's actions as morally acceptable and almost humanitarian, one has to seriously question whether the same positive perception would apply if the Islamic State were to directly contact US families by sending them pictures of their relative's mutilated corpse via social media.[132] To argue that this is just a form of humanitarian outreach clearly ignores the overarching information warfare campaign that Ukraine is waging against Russian society at-large.

According to the IT Army, as of 4 April the Ukrainian government successfully identified 582 corpses with the help of Clearview. The exact figure was likely supplied to the IT Army by the Ukrainian Defense Ministry, Ukraine's intelligence services, or the Ministry of Digital Transformation. None of the Clearview aspects were ever mentioned in the IT Army channel or chat.



Screenshot of the IT Army video posted on April 4, 2022, in the IT Army Telegram channel

On 6 April, the IT Army posted a four-minute video which showed them calling the family of a Russian soldier who allegedly looted around 100 kilograms of goods in Ukraine. The loot was sent via mail from a post office in Moyzr, Belarus, to the town of Chita in the far east of Russia.[133] The IT Army's video identifies the precise weight of the six packages the soldier paid for (totalling around 100 kg), as well as the phone number and address of the recipient (the soldier's brother). The video also shows the CCTV feed of several Russian soldiers with their packages in the same post office. At the beginning of the phone call, the IT Army makes legal threats by pretending to be the FSB. The call ends with the IT Army saying, "we know where you live, where your brother lives, we know everything about your family. You will be responsible for every action that you have done on the territory of Ukraine".[134]

Screenshot of the IT Army video posted on April 6, 2022, in the IT Army Telegram channel

The IT Army subsequently published two similar videos on 8 April and 9 April. In the first one, a Russian soldier sends

[129] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, 18 January 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[130] Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war," *Reuters*, 14 March 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

[131] Mykhailo Federov, Telegram channel, 23 March 2022, https://t.me/zedigital/1399 or https://archive.ph/focdY; Thomas Brewster, "Ukraine Starts Using Facial Recognition To Identify Dead Russians And Tell Their Relatives," *Forbes*, 23 March 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their-relatives/?sh=247648212898.

[132] Ben Gilbert, "Ukraine is using facial recognition tech to identify dead Russian soldiers and inform their families," *Business Insider*, 24 March 2022, https://www.businessinsider.com/ukraine-using-facial-recognition-tech-to-id-dead-russian-soldiers-2022-3?r=US&IR=T or https://archive.ph/3tjiA

[133] IT Army of Ukraine, Telegram channel, 6 April 2022, https://t.me/itarmyofukraine2022/274 or https://archive.ph/4EQ2G.

[134] Ibid.

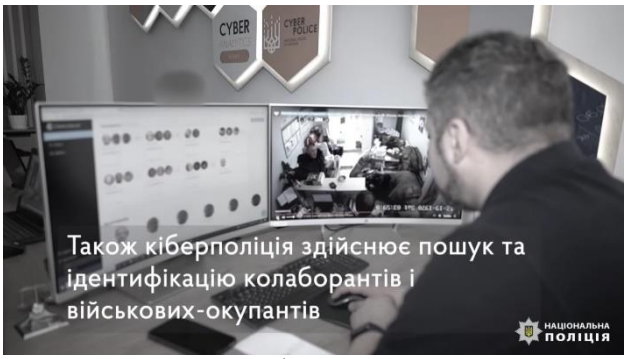
16 kg from the Mozyr post office to his wife in Novosibirsk, Russia.[135] And in the second one, a different Russian soldier sends 63 kg to his wife in Khabarovsk, Russia.[136] The CCTV video is the same in all three videos which suggests that all three Russian soldiers visited the Mozyr post office together.

It is still unclear how the IT Army gained access to all the information necessary to run this operation. How did they know the exact Belarus post office these Russian soldiers would use? Did they breach the CCTV camera in the post office or was the footage given to them by another agency? As of this writing there are no answers to these questions, and none of the operational details of the calls were discussed in the IT Army channel or chat.

What we do know is that on 2 June 2022, two months after the IT Army released the three videos, the Ukrainian Cyberpolice, in conjunction with the Security Service of Ukraine (SBU), utilized the exact CCTV footage to announce the identification of 10 Russian Rosgard soldiers from military unit 6720 that looted the homes of residents in Bucha, Ukraine.[137]

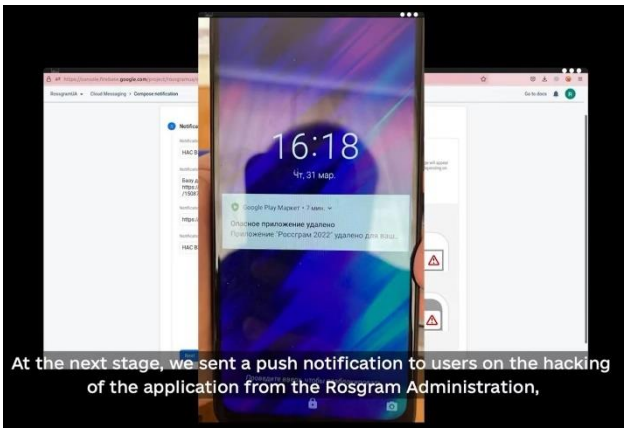
Picture released by the Ukrainian Cyberpolice on June 2, 2022.

While we do not know who got their hands on the CCTV footage first or who oversaw this intelligence gathering operation, we can conclude that either the IT Army supplied the footage to the Cyberpolice and the SBU, or the SBU was overseeing the entire operation and utilized both the IT Army and the Cyberpolice as vehicles for their outreach components, publishing the three calls in April and announcing the soldier idenfications in June. On 16 June, the National Police of Ukraine posted a video on Youtube which showed the usage of Clearview by the Ukrainian Cyberpolice to identify the Russian soldiers in the post office.[138]



Left screen: Clearview user interface / Right screen: CCTV from the Mozyr post office

On 7 April, the IT Army revealed its most sophisticated campaign to date which targeted a Russian Instagram clone called Rossgram. Prior to the official release of the Rossgram app at the end of March, the IT Army claimed to have (1) breached Rossgram's beta sign-up database, (2) created a fake Rossgram app, (3) sent invites to all the beta sign-ups, (4) pushed out notifications to all those who installed the fake app that Rossgram was hacked, and then (5) leaked the beta sign-up database to the public.[139] To date, this is the only hack-and-leak operation for which the IT Army has taken direct credit. None of this was discussed in the IT Army's Telegram channel and chat.



Screenshot of the IT Army video posted on April 7, 2022, in the IT Army Telegram channel

[135] IT Army of Ukraine, "Russian marauders: Parcel in Khabarovsk," Youtube, 8 April 2022, https://www.youtube.com/watch?v=yvH_TLXS4oY.

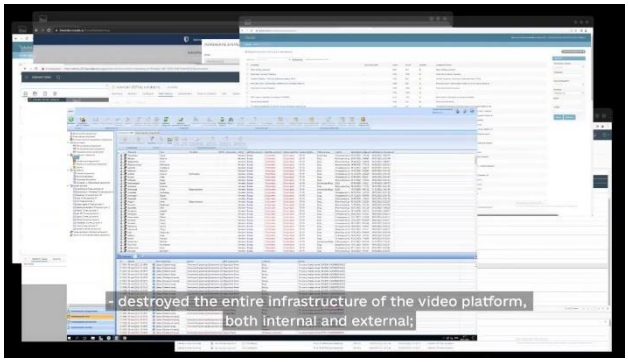
[136] IT Army of Ukraine, "Call to Russian Looters: "Souvenirs" from Ukraine?" Youtube, 9 April 2022, https://www.youtube.com/watch?v=lzdd4PVuETw.

[137] Cyberpolice Ukraine, "Мародерили від білизни до побутової техніки: 10 російським армійцям оголошено підозри," cyberpolice.gov.ua, 2 June 2022, https://cyberpolice.gov.ua/news/maroderyly-vid-bilyzny-do-pobutovoyi-texniky--rosijskym-armijczyam-ogolosheno-pidozry-1559/ or https://archive.ph/9R959; CyberpoliceUA, Telegram channel, 2 June 2022, https://t.me/cyberpolua/1379 or https://archive.ph/TVvRo.

[138] National Police of Ukraine, "Протидія фейкам, пропаганді, хакерським атакам та шахрайству," Youtube, 16 June 2022, https://www.youtube.com/watch?v=CxWn8dvONeg, timestamp: 0:50-0:51

[139] "Russia Unveils Domestic Instagram Competitor 'Rossgram,'" *The Moscow Times*, 29 March 2022, https://web.archive.org/web/20220608133816/https://www.themoscowtimes.com/2022/03/29/russia-unveils-domestic-instagram-competitor-rossgram-a77123; IT Army of Ukraine, Telegram channel, 7 April 2022, https://t.me/itarmyofukraine2022/276 or https://archive.ph/ZpMv7; Stefan Soesanto, Twitter, 7 April 2022, https://web.archive.org/web/20220608133944/https://twitter.com/iiyonite/status/1512001395255357443; Sudo rm -RF, Twitter, 29 March 2022, https://web.archive.org/web/20220608133947/https://twitter.com/sudormRF6/status/1508783518645735429.

On 14 May, the IT Army took credit for the destructive campaign against RuTube.[140] RuTube is a Russian Youtube competitor that was created back in 2006. In mid-March, RuTube's viewership began to skyrocket as Youtube – in reaction to the war in Ukraine — effectively pushed Russian content creators and users off its platform by suspending Google's advertising system in Russia.[141] Given the rapid growth of RuTube and the significant decline of independent media reporting in Russia, the IT Army identified RuTube as the "main information center for Russian false propaganda".[142] Timed to coincide with Russia's Victory Day celebrations on 9 May 2022, the IT Army — with the help of "two specialists" — subsequently ran a destructive campaign against RuTube starting the night of 8 May. According to the IT Army's video, the campaign successfully (a) changed all administrator passwords, (b) blocked all the access cards that were needed to enter and exit RuTube's server rooms, (c) deleted "dozens of petabytes of information", (d) "demolished all systems – virtualization, databases, content, converter, content search systems, advertising module, load distribution systems and management of the entire infrastructure", and (e) exfiltrated internal information from the computers of the RuTube administrators and employees.[143] The attack against RuTube is the first ever destructive campaign for which the IT Army has taken credit.



Screenshot of the IT Army video posted on May 14, 2022, in the IT Army Telegram channel

RuTube remained offline for almost three days with partial access being restored on 11 May: Recovery commenced in stages.[144] According to RuTube's official Telegram channel, Russian cybersecurity company Positive Technologies helped to investigate and remediate the attack.[145] RuTube also explained that "there have been many attacks on RUTUBE that have been successfully localized. However, the 9 May incident was of a different level of complexity. The readiness of the infrastructure for such a targeted attack can only be established by encountering it".[146] On 14 May, the site seemed to have been fully restored from its backups.

As of this writing, it is still unknown how large the IT Army's in-house team is, or who exactly is tasking and feeding them information. The in-house team likely consists of members located in Ukraine and Ukrainians living abroad. As of this writing, the IT Army has open vacancies for pentesters, desktop developers, hackers, system administrators, graphic designers, and, most importantly, connoisseurs of English. The vacancy site describes the in-house team's tasks as "hacking enemy resources, spreading viruses, creating phishing sites, and inflicting maximum damage on the [Russian] economy and other public spheres".[147]

Curiously, on 18 May, the IT Army channel put out a crowdsourcing call for information, stating that "we need your help in finding databases with phone numbers of private individuals and legal entities from the occupied Crimea as well as Russian regions next to the Ukrainian border (Briansk, Kursk, Belgorod). You can send this information to itarmyua@gmail[.]com".[148] Four days later, the IT Army thanked everyone that sent in information, and put out a second request for help, stating, "we need your help in finding databases with the phone numbers of Russians who fall under one of the following categories: (a) "young people who have radical views and are into working out (e.g. bouncers, members of martial arts groups)", (b) "draftee (people who might be conscripted for military service)", (c) "students", and (d) "military service offices employees and their relatives".[149]

As of this writing it is still unknown for what purpose the IT Army has been collecting this information. It might end up being used by the in-house team for one of their upcoming campaigns, it could be forwarded to the Internet

[140] IT Army of Ukraine, Telegram channel, 14 May 2022, https://t.me/itarmyofukraine2022/349 or https://archive.ph/U0H43.

[141] Similarweb, "rutube.ru Ranking," accessed 8 June, https://www.similarweb.com/website/rutube.ru/#ranking; Youtube Help, "YouTube Partner Program overview & eligibility," accessed 8 June, https://support.google.com/youtube/answer/72851?hl=en&ref_topic=9153642.

[142] IT Army of Ukraine, Telegram channel, 14 May 2022, https://t.me/itarmyofukraine2022/349 or https://archive.ph/U0H43, time stamp: 00:29.

[143] IT Army of Ukraine, Telegram channel, 14 May 2022, https://t.me/itarmyofukraine2022/349 or https://archive.ph/U0H43, time stamp: 01:26-02:11; Sudo rm -RF, Twitter, 10 May 2022, https://web.archive.org/web/20220608105911/https://twitter.com/sudormRF6/status/1524143579140083715.

[144] Rutube, Telegram channel, 10 May 2022, https://t.me/rutube/4177 or https://archive.ph/jBcEV; Rutube, Telegram channel, 11 May 2022, https://t.me/rutube/4180 or https://archive.ph/YcSeH; Rutube, Telegram channel, 11 May 2022, https://t.me/rutube/4181 or https://archive.ph/FSaUc.

[145] Rutube, Telegram channel, 10 May 2022, https://t.me/rutube/4179 or https://archive.ph/018cq; Rutube, Telegram channel, 11 May 2022, https://t.me/rutube/4180 or https://archive.ph/YcSeH.

[146] Rutube, Telegram channel, 12 May 2022, https://t.me/rutube/4183 or https://archive.ph/397ev.

[147] IT Army of Ukraine, website, vacancies, accessed 8 June, https://web.archive.org/web/20220608134307/https://itarmy.com.ua/vacancies/?lang=en.

[148] IT Army of Ukraine, Telegram channel, 18 May 2022, https://t.me/itarmyofukraine2022/364 or https://archive.ph/KMKTj.

[149] IT Army of Ukraine, Telegram channel, 22 May 2022, https://t.me/itarmyofukraine2022/375 or https://archive.ph/LPpT0.

Forces of Ukraine for an information warfare operation, or it could even be utilized to organize Russians in Russia to act against the Russian state apparatus. Time will tell.

6 Where are Ukraine's intel services?

The IT Army is the main hub for Ukraine's "offensive" response in cyberspace in reaction to the Russian invasion. Parallel to this cyber effort, the Internet Forces of Ukraine were stood up on 28 February to wage the nation's "offensive" campaign in the information warfare domain. The focus of the Internet Forces is on organizing political pressure campaigns abroad and disseminating Ukrainian war propaganda via social media, including Telegram, VKontakte, Discord, and Reddit. The Ministry of Digital Transformation has taken public credit for establishing both the IT Army and the Internet Forces of Ukraine on 10 March.[150]

As it currently stands, the IT Army and the Internet Forces are publicly portrayed as two civilian-led government projects that function entirely separately from Ukraine's military command structure and maintain no links whatsoever to the nation's intelligence services. From a purely institutional point of view, however, 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. For Ukraine's defense and intelligence services to roll their thumbs and let the IT Army and Internet Forces conduct operations freely and independently – particularly during war time – seems to be not only an analytical stretch but would highly likely also lead to strategic confusion and tactical interference with the defense and intelligence services' own operations in cyberspace.

It is also questionable whether the Ministry of Digital Transformation has the necessary in-house skills and knowledge that underpins the cyber and information warfare operations the IT Army and Internet Forces have been conducting. Talking to *Wired*, Anton Melnyk, who is an advisor to the Ministry of Digital Transformation, explained that "we have restructured the Ministry of Digital Transformation into a clear military organization".[151] Similarly, speaking to *Politico* on 8 March, Deputy Minister of Digital Transformation Oleksandr Bornyakov noted that "we are the first in the world to introduce this new warfare. And it's powerful, yet simple at the same time. […] It's impossible to disrupt it or break it down".[152]

Back in March 2022, Dina Temple-Raston interviewed one of the eight administrators of the IT Army channel for *The Record*. Probably the most interesting exchange occurred right at the beginning when Dina asked: "Do you have a military background?" The administrator answered, "Um, sort of […] It's not the questions I can answer you fully because it may lead to a better understanding of what kind of person I am".[153] While we cannot be certain, we can somewhat infer that any statement on having served in the three main service branches would not have provided peculiar insights – i.e., the statement "I was in the Navy" could mean anything from being a cook to a naval demolition specialist. But the outright refusal to say anything may hint at an intelligence background. Similarly, it is highly unlikely that an unvetted random person on the internet is being entrusted with the role of administrating the IT Army channel and overseeing a community of close to 300,000 subscribers to organize Bornyakov's "new warfare". At a minimum one would expect some level of social media campaigning or government coordination experience, and at a maximum an intelligence/military background in cyber or information warfare.

Interestingly, from the Russian perspective, the IT Army and Internet Forces likely maintain close relations – or might even be extensions – of Ukraine's 72nd Center for Informational and Psychological Operations in Brovary/Kyiv. The 72nd Center was stood up back in 2003 in Sevastopol as part of Ukraine's Special Operations Forces and was one of the last military units that resisted the Russian occupation of Crimea in 2014. Until recently, the 72nd was Ukraine's main center that specialized in information and psychological operations.[154] Very little is publicly known about the internal structure and operations the 72nd has conducted in the past, and given the current war

[150] KMU.gov.ua, "Мінцифри бореться з ворогом на цифровому фронті," 10 March 2022, https://web.archive.org/web/20220310141242/https://www.kmu.gov.ua/news/mincifri-boretsya-z-vorogom-na-cifrovomu-fronti.

[151] Simonite and Volpicelli, "Ukraine's Digital Ministry Is a Formidable War Machine."

[152] Elise Labott, "'We Are the First in the World to Introduce This New Warfare': Ukraine's Digital Battle Against Russia," *Politico*, 8 March 2022, https://web.archive.org/web/20220608135145/https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880.

[153] Dina Temple-Raston, "Fighting Russia with computers, not rifles," *The Record*, 22 March 2022, https://web.archive.org/web/20220608135214/https://therecord.media/fighting-russia-with-computers-not-rifles/.

[154] There are also three smaller centers that specialize in information and psychological operations: the 16th is based in Huiva/Zhytomyr, the 74th in Lviv, and the 83rd in Odessa.

context, it is rather difficult to distinguish between reliable new information and Russian war propaganda.[155] For example, according to the Russian International Affairs Council, the 72nd is not only involved in intelligence, subversion, and counterintelligence activities, but also conducts "propaganda information campaigns in telecommunications networks and the Internet, and, together with the [Security Service of Ukraine], coordinate the activities of Ukrainian patriotic hacker groups, volunteer information communities and Internet resources".[156]

What we definitely do know is that on 1 March the Russian Defense Ministry proclaimed that "information attacks on Russia are carried out by the 72nd Main Center for Information and Psychological Operations of the Armed Forces of Ukraine, together with the cyber operations units of the SBU, using hardware and software systems and communication facilities in Kyiv".[157] The Ministry went on to explain that "in order to thwart informational attacks against Russia, [Russian forces] will strike technological objects of the [Security Service of Ukraine] and the 72nd Main [Psychological Operations] Center in Kiev".[158] On 2 March, Russian air strikes took out the SBU's headquarter, the 72nd Center, as well as a building that housed the control room of Kyiv's TV tower.[159] Notably, as of this writing, no Russian airstrike has been directed at the building of the Ministry of Digital Transformation.

Source: https://tass.com/defense/1414709

Another somewhat related piece to the puzzle appeared on 7 March, when cybersecurity consultant Jeffrey Carr published an article on his substack *Inside Cyber Warfare*, which claimed that the Beloyarsk Nuclear Power Plant in Zarechny, Russia, was breached by cyber operators from the Main Intelligence Department of the Ukrainian Ministry of Defense (GURMO). According to Carr, GURMO exfiltrated "a large amount of data including contracts, architectural diagrams, alarm system configurations, set-up instructions for control system parts".[160] It is highly questionable whether Carr ought to be considered a reliable source. As he himself explains, "the problem was that journalists wanted to speak to GURMO and that was off the table […]. They could speak with me because I was the only person who the GURMO team would directly speak to".[161] Given the unverifiability of Carr's claims, journalists were rightfully not willing to put their reputation on the line for a single-sourced story. As of this writing, Carr has published 16 additional pieces claiming that GURMO breached Roscosmos, Gazprom, the communication servers of the Black Fleet, as well as the FSB's Special Operations Unit 607. None of these claims have been verified. In early April, Carr even went as far as insinuating that GURMO gained access to Gazprom's pressurization controls, supposedly leading to the physical rupture and fire at two Russian pipelines.[162] There is zero evidence that supports Carr's story. What is similarly problematic is that Carr claims to be in possession of the complete data leaks that GURMO allegedly exfiltrated, but only paying subscribers to his substack are allowed access. Why does he not approach DDoSecrets like Anonymous has frequently done to publish its data leaks? Why is GURMO only using Carr as their public representative and no one else – not even the IT Army, Internet Forces, or any of the well-established professional journalists covering cyber? Given the absence of logical answers, Carr's substack ought to be read with great caution. Having said that, Carr's reporting does present an easy answer to the question as to

[155] See for example: Marina Sovina, "В Крыму опровергли информацию о массовой мобилизации," *Lenta*, 26 March 2022, https://lenta.ru/news/2022/03/26/krim/ or https://archive.ph/ddzNi; Spravdi.gov.ua, "General Mizintsev's Bloody Precaution. How Russian propaganda works during the war," 7 April 2022, https://spravdi.gov.ua/en/general-mizintsevs-bloody-precaution-how-russian-propaganda-works-during-the-war/.

[156] RIAC, "Организация кибербезопасности Украины," accessed 8 June, https://web.archive.org/web/20220608134819/https://russiancouncil.ru/cyberukraine-org.

[157] Svoboda, "Минобороны России анонсировало удары по объектам СБУ в Киеве," 1 March 2022, https://www.svoboda.org/a/minoborony-rossii-anonsirovalo-udary-po-obektam-sbu-v-kieve/31730350.html. Please note that on February 24, the first day of the invasion, Russian news outlets speculated that the 72nd Center was hit by the initial barrage of Russian airstrikes. See: RIA, "Очевидцы: в районе военных частей на окраине Киева поднимается дым," 24 February 2022, https://web.archive.org/web/20220608134747/https://ria.ru/20220224/dym-1774674819.html.

[158] TASS, "Russian Defense Ministry warns about strikes being prepared on military sites in Kiev," 1 March 2022, https://tass.com/defense/1414199 or https://archive.ph/8x3nO.

[159] TASS, "Russian Armed Forces hit SBU, 72nd Psychological Operations Center objects in Kiev," 2 March 2022, https://tass.com/defense/1414709 or https://archive.ph/9vaqx. In the aftermath of the air strikes, the Ukrainian government asserted that the holocaust memorial complex Babyn Yar was also hit, sparking outrage in western media outlets and Jewish organizations. According to CNN national security correspondent Alex Marquardt, on 2 March the main memorial was not damaged (see: https://web.archive.org/web/20220608134808/https://transcripts.cnn.com/show/nday/date/2022-03-02/segment/05).

[160] Jeffrey Carr, "Russia's Beloyarsk Nuclear Power Plant has been breached by a GURMO Cyber unit," *Inside Cyber Warfare*, 7 March 2022, https://web.archive.org/web/20220608110016/https://jeffreycarr.substack.com/p/russias-beloyarsk-nuclear-power-plant?s=r.

[161] Jeffrey Carr, "My experience working with Ukraine's Offensive Cyber Team," *O'Reilly*, 22 March 2022, https://www.oreilly.com/radar/d-day-in-kyiv/ or https://archive.ph/gTd1x.

[162] Jeffrey Carr, "GURMO Hackers Go Kinetic Against Gazprom - Two Pipeline Fires So Far," *Inside Cyber Warfare*, 5 April 2022, https://web.archive.org/web/20220608105903/https://jeffreycarr.substack.com/p/gurmo-hackers-go-kinetic-against?s=r.

what Ukraine's intelligence services have been up to in cyberspace. If we treat Carr's pieces at face value, then GURMO is primarily focusing on hack-and-leak operations that have even less immediate impact on the course of the war than those conducted by Anonymous and other hacking groups since the start of the invasion.[163] Similarly, if viewed in relation to the strategic and public impact the IT Army and Internet Forces have had on Russian society, private companies, and foreign governments, then GURMO's activities are close to irrelevant.

The absence of known activities by Cloud Atlas – the only advanced persistent threat (APT) actor that might be of Ukrainian origin – amidst the Russian invasion is another mystery that has not yet been solved.[164] Overall, there are currently no good answers to the question of what Ukraine's intelligence and defense agencies are doing offensively in cyberspace. The only logical answer with the current evidence at hand is that the Ukrainian intelligence services are likely deeply intertwined with the IT Army's DDoS targeting and tasking flow, the Internet Forces' information warfare activities, and the IT Army's in-house operations. Assertions that Ukrainian intelligence and defense agencies are not involved at all in any of these activities are either naïve or – at this point – wilfully ignorant.

7 The IT Army and External Groups

Open-source intelligence researcher CyberKnow has assembled the most comprehensive overview of all the different hacking groups/individuals that have popped up since the Russian invasion.[165] On 1 May, CyberKnow identified 74 active groups/individuals, 46 pro-Ukraine, 26 pro-Russia, and two whose allegiance is unknown.[166]

Apart from the IT Army's DDoS cooperation with a variety of groups on Telegram, there is very little known about how the IT Army views groups such as the Belarusian Cyber Partisans and the numerous sub-groups that are operating under the banner of Anonymous.

The Partisans were formed back in September 2020 in reaction to the protests and subsequent violent crackdown following the contested presidential election in Belarus. The group's first known public hack was the defacement of the website of the Belarusian Presidency on 2 September 2020. Only nine days later, the Partisans conducted one of their most impactful hack-and-leak operation to date by sharing a vast database of Belarusian law enforcement officers with NEXTA, which has become the biggest Russian-speaking Telegram channel/media outlet covering the protests in Belarus. In August 2021, the Partisans became one of the three founding organizations of the Belarusian resistance alliance Suprativ. The other two are the Flying Storks, who are conducting resistant activities outside of cyberspace, and the People's Self-Defense Squads, who are publishing training videos and self-defense instructions. In the context of the war in Ukraine, the Partisans rose to international fame when they ran a ransomware campaign against the IT systems of Belarusian Railways on 24 January 2022 to disrupt the movement of Russian tanks and equipment.[167]

Anonymous

By contrast, Anonymous is an umbrella term for a decentralized collection of activities that feed into the global Anonymous movement and its diffuse ideology.[168] Following the Russian invasion of Ukraine, several prominent Anonymous information hubs on social media accounts announced the beginning of Operation Russia or #OpRussia.[169] Generally speaking, each Anonymous group/personality conducts their own operations. Occasionally, Anonymous groups/personalities loosely run operations together, and sometimes they might even breach the

[163] Kevin Collier, "Hackers flood internet with what they say are Russian companies' files," *NBC News*, 5 April 2022, https://web.archive.org/web/20220608110222/https://www.nbcnews.com/tech/security/hackers-flood-internet-say-are-russian-companies-files-rcna21853.

[164] Joe Slowik, "Current Events to Widespread Campaigns: Pivoting from Samples to Identify Activity," *First*, 14 December 2020, https://web.archive.org/web/20220608110326/https://www.first.org/blog/20201214-Current_Events_to_Widespread_Campaigns; Joe Slowik, "The Continuous Conundrum of Cloud Atlas," *Domaintools*, 25 February 2021, https://web.archive.org/web/20220608110234/https://www.domaintools.com/resources/blog/the-continuous-conundrum-of-cloud-atlas.

[165] Cyberknow, "Cyberknow," *Medium*, accessed 8 June, https://web.archive.org/web/20220608110420/https://cyberknow.medium.com/.

[166] Cyberknow, "Update 13. 2022 Russia-Ukraine war — Cyber group tracker. May 1," *Medium*, 1 May 2022, https://web.archive.org/web/20220608110359/https://cyberknow.medium.com/update-13-2022-russia-ukraine-war-cyber-group-tracker-may-1-f0188bc96af3.

[167] Andy Greenberg, "Why the Belarus Railways Hack Marks a First for Ransomware," *Wired*, 25 January 2022, https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/; Belarusian Cyber Partisans, Twitter, 24 January 2022, https://web.archive.org/web/20220608110648/https://twitter.com/cpartisans/status/1485615555017117700.

[168] Writing in July 2015, Biella Coleman aptly described Anonymous' metamorphosis as one "from trolling misfits to the misfits of activism." See: Gabriella Coleman, "Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous," (Verso: New York, 2015), p. 8.

[169] YourAnonNews, Twitter, 26 February 2022, https://web.archive.org/web/20220608110756/https://twitter.com/YourAnonNews/status/1497574730282541060; Anon2World, "Anonymous: OpRussia," Youtube, 27 February 2022, https://www.youtube.com/watch?v=kcb2yudJ29c.

same target during similar time frames by pure coincidence.[170] As of this writing, OpRussia has primarily consisted of DDoS attacks and hack-and-leak operations against Russian private companies and government digital infrastructure. What is important to stress is that each Anonymous group/personality has its own political motive and ethical reasoning. Sometimes these motives can generate initial approval and subsequent severe backlash from other Anonymous groups, as was the case when an Anonymous personality known as I_am_Mr_Grey (about 8,000 Twitter followers) announced Operation Falling Star in early April 2022. Grey essentially threatened that Anonymous would hack satellites in orbit and make them fall out of the sky. In a now deleted tweet with a video, Grey declared, "Dear NATO / UN / Putin – a message for you. We give you the rise of operation Falling Star. Should Putin attempt a second invasion and you NATO / UN does nothing, this SHALL be your fate".[171] Grey was subsequently ridiculed and ostracized to the point that he grovelingly apologized for his behavior.

The first item to note is that both the Belarusian Cyber Partisans and almost all groups operating under the banner of Anonymous are primarily active on Twitter. The IT Army by contrast exclusively operates on Telegram. That being said, the closest to an official IT Army representative on Twitter is an account called sudo rm -RF (@sudormRF6), who says that he represents the "Ukrainian Cyber Front".[172] The connection between sudo rm -RF and the IT Army consists of at least three data points. First, sudo rm -RF posted the Rossgram beta-sign up database on 29 March 2022, – one week prior to the IT Army releasing its video on Rossgram – using the file sharing service Mega[.]nz.[173] Second, sudo rm -RF posted several screenshots of RuTube's internal folders, documents, and source code on 10 May - four days prior to the IT Army posting its video about RuTube.[174] And third, the sudo rm -RF account appears for eight seconds in the IT Army's RuTube video, during which the narrator discusses "gradually publishing [RuTube internal documents] on the Mega[.]nz file sharing service".[175]

Except for sudo rm -RF, all other accounts that claim to represent the IT Army of Ukraine on Twitter are neither affiliated nor officially endorsed by the IT Army. This includes the 45,600 or so follower strong ITarmyUA account which many individuals in the Anonymous movement portrayed as being the official IT Army Twitter account. In fact, almost every time Anonymous claims to have cooperated with the IT Army they tag the ITarmyUA account in their tweets.[176] Thus, when Twitter suspended ITarmyUA on 29 April, thousands of Twitter users viewed this as an act against Ukraine and fundamentally as political censorship.[177]

For anyone that bothered to take a closer look, it was immediately evident that ITArmyUA was a rebranded account created back in August 2018 that changed its user handle and scrubbed all its tweets prior to March 2022. No one in the IT Army's Telegram channel ever mentioned or cared about the ITArmyUA account being suspended on Twitter. The official IT Army website does not link to the ITarmyUA account, and neither Mykhailo Federov nor the Ministry of Digital Transformation follows the ITarmyUA account on Twitter.

So how does Anonymous' outrage fit into the bigger picture? Looking at the dynamics and possible motives, it is highly likely that someone identifying with the Anonymous movement rebranded their account to pretend to be the IT Army on Twitter. The ITarmyUA account was then subsequently hyped by numerous Anonymous accounts to gain a massive Twitter following out of nowhere. The account was then utilized to provide legitimacy to the claims that Anonymous was actively cooperating with the IT Army, and by extension created the illusion that the Ukrainian government endorsed Anonymous' actions.

Anonymous' desperate hunt for legitimacy and official government recognition has even led some groups to insert the Anonymous logo into copies of the IT Army's official videos, and others went so far as to proclaim themselves to be the official international chapter of the IT

---

[170] For example, in mid-April, 20202, three Anonymous groups/personalities (DepaixPorteur, NB65, and an unknown Anonymous group) targeted SSK Gaz during the same time frame. All three submitted their SSKGaz files to DDoSecrets for publication. As DDoSecrets put it, "Three different hacktivist sources submitted files from Gazregion at approximately the same time, with some overlap." See: DDoSecrets, "Gazregion," accessed 8 June, https://ddosecrets.com/wiki/Gazregion.

[171] I_Am_Mr_Grey, Twitter, 6 April 2022, https://web.archive.org/web/20220406183036/https://twitter.com/IAmMrGrey2/status/1511769272833515524.

[172] Sudo rm -RF, Twitter, 2 March 2022, https://web.archive.org/web/20220516124424/https://twitter.com/sudormRF6/status/1499117121040752641; Note: "sudo rm -rf /" is a Linux command that essentially wipes your entire Linux system," see: Linux Stans, "sudo rm -rf /: The Command You Should Never Run," 19 Feburary 2022, https://linuxstans.com/sudo-rm-rf/.

[173] Sudo rm -RF, Twitter, 29 March 2022, https://web.archive.org/web/20220329123018/https://twitter.com/sudormRF6/status/1508783518645735429.

[174] Sudo rm -RF, Twitter, 10 May 2022, https://web.archive.org/web/20220608111028/https://twitter.com/sudormRF6/status/1524143588019421184.

[175] IT Army of Ukraine, Telegram channel, 14 May 2022, https://t.me/itarmyofukraine2022/349 or https://archive.ph/U0H43, time stamp: 02:27-02:35.

[176] PucksReturn, Twitter, 28 April 2022, https://web.archive.org/web/20220608110810/https://twitter.com/PucksReturn/status/1519495471647047680.

[177] PucksReturn, Twitter, 29 April 2022, https://web.archive.org/web/20220608111103/https://twitter.com/PucksReturn/status/1520082201093804032; AnonOPsSE, Twitter, 30 April 2022, https://web.archive.org/web/20220608110953/https://twitter.com/AnonOpsSE/status/1520361102323953665.

Army of Ukraine.[178] None of these claims has ever been acknowledged by the IT Army. In fact, the IT Army's Telegram channel has only ever once used the word "anonymous" when they thanked the Telegram group Anonymous-Ukraine on 4 April for their DDoS cooperation.

Overall, the IT Army has shown little interest in officially displaying any closeness to the Anonymous movement. This behaviour is likely due to (a) Anonymous' decentralized nature and not knowing who is speaking on whose behalf, and (b) Anonymous' reputation as a loose cannon in general, where every group and individual does what they want for the sake of social media clout and public attention. As of this writing it is unknown whether the IT Army's in-house team has occasionally cooperated with groups that are close to Anonymous. Repeated email inquiries to the IT Army to verify claims made by a handful of groups (including BeeHiveCybersec) have gone unanswered.

Belarusian Cyber Partisans

Curiously, the Belarusian Cyber Partisans have also faced the same unresponsiveness from the IT Army. On 18 March, the Partisans wrote on Twitter that "we are willing to support [the IT Army] with intelligence, tools and ops. Sent them an email and then twitted about it. We did not get a reply from them as of yet".[179] When asked again on 29 April, the Partisans explained that we "haven't managed to get a direct contact unfortunately".[180] As of this writing, the Partisans appear to have been unable to connect with the IT Army.

The IT Army did target Belarusian sites on 27 February, when the channel announced 43 different sites to DDoS, including websites of the Belarusian government, media, banks, and industrial companies.[181] The only other two instances in which the IT Army did so, was on 20 March – against the Belarusian site of Bitrix24, which is a cloud customer relationship management company headquartered in Virgina, US.[182] And on 5 April, the IT Army targeted cdek[.]by – which is the Belarusian site of the Russian international express delivery company CDEK.[183] Since 5 April, no Belarusian sites have been targeted by the IT Army. It is unclear whether this change is a deliberate restriction based on internal decisions, or simply an evolutionary process by which the IT Army has come to focus solely on Russia.

The IT Army's reluctance to talk to the Partisans might be following the same logic as it does vis-a-vis Anonymous. The IT Army does not have good answers to (a) who exactly the individuals are that make up the Partisans, (b) whether the IT Army can trust them, (c) what the Partisans underlying political motives are – given that they are part of the Belarusian resistance alliance Suprativ, (d) whether an IT Army-Partisan cooperation in cyberspace could be politically viewed as the Ukrainian government cooperating with the Belarusian opposition in exile, and (e) what the IT Army's options are if the Partisans go off script with their activities.

Overall, the hybrid setup the IT Army has mastered requires a healthy sense of paranoia and the need to take operational security extremely seriously – to guard against Russian infiltrators and information breaches. Particularly in times of war, discerning between who is a friend, a foe, and everything else in between is an inherently complicated task.

IPStress

One curious external cooperation popped up in early May when the itarmy[.]com].[ua] website began to display its one and only partner on the bottom of its site: IPStress[.]in.[184] According to IPStress itself, they are the best IP booter stresser that "can down any game server such as ovh, nfo, fivem servers etc. Bypassing every protection such as cloudflare with our blazingfast methods. Buy now and enjoy the strong power from our botnets as well".[185] That self-description got a bit weird, when in early 2022 the IPStress[.]in website started to use Cloudflare's DDoS protection service.[186]

---

[178] Anonymous, "A Message from IT Army of Ukraine and Anonymous," Youtube, 25 April 2022, https://www.youtube.com/watch?v=lfNf336Y5lY; WhiteDeathCyber, Twitter, 18 April 2022, https://web.archive.org/web/20220608111544/https://twitter.com/WhiteDeathCyber/status/1516010603843837957.

[179] Belarusian Cyber Partisans, Twitter, 18 March 2022, https://web.archive.org/web/20220608111705/https://twitter.com/cpartisans/status/1504801050444058624.

[180] Belarusian Cyber Partisans, Twitter, 29 April 2022, https://web.archive.org/web/20220608111733/https://twitter.com/cpartisans/status/1520150809912266759.

[181] IT Army of Ukraine, Telegram channel, 27 February 2022, https://t.me/itarmyofukraine2022/27 or https://archive.ph/xtC1p.

[182] IT Army of Ukraine, Telegram channel, 20 March 2022, https://t.me/itarmyofukraine2022/221 or https://archive.ph/sHfGY.

[183] IT Army of Ukraine, Telegram channel, 5 April 2022, https://t.me/itarmyofukraine2022/269 or https://archive.ph/Tne61.

[184] IT Army of Ukraine, website, 9 May 2022, https://web.archive.org/web/20220509132136/https://itarmy.com.ua/.

[185] IP Stress, website, 19 December 2021, https://web.archive.org/web/20211219144712/https://ipstress.in/.

[186] IP Stress, website, 31 May 2022, https://web.archive.org/web/20220331084353/http://ipstress.in/.

Screenshot of itarmy[.]com[.]ua on May 9, 2022.

On 31 May 2022, the FBI and the US Department of Justice announced the seizure of three internet domains: weleakinfo[.]to, ovhbooter[.]com, and ipstress[.]in. In the DoJ's press release, US Attorney of the District of Columbia Matthew M. Graves explained that ipstress and ovhbooter "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".[187]

The simultaneous take down of all three domains and police raids in several locations suggests that this was the culmination of a months – if not year – long criminal investigation. Thus, the take down of IPStress[.]in did not occur in response to their partnership with the IT Army. Nonetheless it is rather disturbing that the IT Army – a Ukraine government-created entity – was willing to form and openly advertise its partnership with a cybercriminal DDoS enterprise. As of this writing, the IT Army website has changed its official partner to the hosting service ukraine[.]com[.]ua.

Screenshot of the ipstress[.]in website on June 2, 2022

As of June 7, 2022, IPStress[.]in is still mentioned on the IT Army website under the official English translation for the section on "Friends and Partners of the IT Army of Ukraine".[188]

On June 10, 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".[189]

8 Conclusion

The IT Army of Ukraine is a unique and smart construct whose organizational setup and operational impact will likely inform the art of cyber and information warfare in future conflicts. On the public side, the IT Army serves as a vessel that allows the Ukrainian government to utilize volunteers from around the world in its persistent DDoS activities against Russian government and company websites. As of 7 June 2022, this includes 662 targets. On the non-public side, the IT Army's in-house team likely maintains deep links to – or largely consists of – the Ukrainian defense and intelligence services.

Overall, both Kyiv and the Ukrainian IT community at large have shown the world what digital diplomacy on steroids looks like. Their conduct has collapsed entire pillars of existing legal frameworks regarding norms and rules for state behaviour in cyberspace and has taken apart the illusion of separating the defense of Ukraine from Ukrainian companies and citizen living abroad. As of this writing, EU and NATO member states have equally failed to adapt to – or even grasp – what the IT Army really is. Western observers and governments still believe that it is just a collection of random volunteers conducting meaningless DDoS attacks against Russian websites. They have so far failed to see the underlying organizational structure, operational conduct, and wider ecosystem that underpins the IT Army and Ukraine's fight in the cyber and information domain. For better or worse, continuing to ignore the essence of the IT Army will wreak havoc on the future

[187] US Department of Justice, "WeLeakInfo.to and Related Domain Names Seized," 31 May 2022, https://www.justice.gov/usao-dc/pr/weleakinfoto-and-related-domain-names-seized or https://archive.ph/X5wAe.

[188] IT Army of Ukraine, "Friends and Partners of IT Army of Ukraine," itarmy.com.ua, 7 June 2022, https://web.archive.org/web/20220607134600/https://itarmy.com.ua/partners/?lang=en.

[189] Ministry of Foreign Affairs of the Russian Federartion, "Answer of the Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia A.V. Krutskikh to a media question about attacks on Russian critical infrastructure," 9 June 2022, https://www.mid.ru/ru/foreign_policy/news/1817019/ or https://archive.ph/8U6CN.

stability of cyberspace and with it the national security landscape in Europe and beyond.

There are many questions this report leaves unanswered or can only answer in varying degrees of certainty. Time will tell how the IT Army evolves from here on out and whether history will judge this report as being both balanced and objective.

Some questions this report has not touched upon might be of interest to future research and policy discussions including:

(1) How is it possible that the official IT Army website (itarmy[.]com[.]ua) and Cyber Palyanits (cyberarmy[.]com.ua) are protected by Cloudflare's anti-DDoS service? On both sites users can find an assortment of DDoS tools and instructions. It seems rather odd that an anti-DDoS service like Cloudflare is protecting the very sites that are organizing the most impactful DDoS activities amidst the Ukraine war.

(2) How is it possible that the IT Army's official email account and application forms are hosted by Google, when the itarmy[.]com[.]ua site includes detailed instructions on how to misuse Google's Cloud Servers for DDoS attacks?[190] Does Google have a policy in place to deal with belligerents using its products in the context of an international armed conflict?

(3) Does GitHub – and by extension Microsoft – have a policy in place to take down repositories/tooling specifically designed for users worldwide to participate in an international armed conflict? As of this writing, senior Microsoft executives have been publicly preaching about preventing cyberwar – while actively helping Ukraine defending its networks – yet none of the GitHub repositories mentioned in this report seems to violate GitHub's terms of service.

(4) What are the economics of the IT Army and the ecosystem around it? Are cryptocurrency donations, influencer support, and holders of Hacken's various tokens a major source of revenue to improve the IT Army's DDoS infrastructure both in and outside Ukraine?

(5) And what political prescedents are US software companies such as Clearview, Starlink, and maybe soon Palantir setting by offering their novel technologies and infrastructure to one belligerent in an international armed conflict? In the context of the Ukraine war, it might be easy for company executives to decide which belligerent to support. But what happens when that assessment runs counter to US foreign policy interests? Also, how should other governments – particularly those in Europe – view the conduct of these companies? Should they be seen as extensions of US foreign policy? Or are they independent actors? And if so, what strategic interests, foreign policies, and legal and ethical considerations underpins the conduct of those companies?

[190] IT Army of Ukraine, "Instructions for Deploying Virtual Machines", itarmy.com.ua, 7 June 2022, https://web.archive.org/web/20220607144831/https://itarmy.com.ua/vps/.

List of Acronyms

AF	Urban dictionary: “Short for ‘as fuck’ used with an adjective to demonstrate something or someone as being the maximum level of that description”
APT	Advanced Persistent Threat
AWS	Amazon Web Services
CCTV	Closed-circuit Television
CET	Central European Time
CIS	Commonwealth of Independent States
CSS	Center for Security Studies
Db1000n	Death by 1000 needles
DDoS	Distributed Denial of Service
DNS	Domain Name Service
EGAIS	*Единой государственной автоматизированной информсистемы учета алкоголя* / Unified State Automated Information System for Alcohol Accounting
FSB	*Федеральная служба безопасности Российской Федерации* / Federal Security Service of the Russian Federation
GURMO	*Головне управління розвідки Міністерства оборони України* / Main Intelligence Directorate of the Ministry of Defence of Ukraine
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
LFI	Local File Execution
NFT	Non-fungible Token
NGO	Non-governmental Organization
OS	Operating System
R&D	Research and Development
RCE	Remote Code Execution
RFI	Remote File Execution
RIAC	Russian International Affairs Council
SBU	*Служба безпеки України* / Security Service Ukraine
SCADA	Supervisory Control and Data Acquisition
SQLi	Structured Query Language (SQL) Injection
Sudo rm -RF /	Linux command that essentially wipes the entire system
TGstat	Telegram Stat
UA	Ukraine
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

About the Author

Stefan Soesanto is a Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich. Stefan works closely with the Swiss Defense Department. Among others, his writings have been published by the Cyber Defense Review, Air University, Lawfare, the Royal Institute Elcano, the Konrad-Adenauer Stiftung, Defense One, and the Council on Foreign Relations.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.