Cyber-enabled Influence Operations

The case of the Belarusian Cyber Partisans

Peter Schrijver MA and Prof. Dr. Paul Ducheine*

The Belarusian Cyber Partisans (BCP) have opposed the authoritarian government of Belarus since 2020 through cyber attacks. They have hacked government and police databases, revealing sensitive information about government personnel. One notable event was their hack of the Belarusian railway system in early 2022, which disrupted the Russian military build-up to the large-scale invasion of Ukraine. To this day, the Cyber Partisans continue to challenge the regime of President Lukashenko and Russian presence and influence in Belarus. An analysis offers more conceptual clarity on the effects sought by non-state groups like the BCP, and thereby on how the Cyber Partisans should be labelled.

One month before the full-scale Russian invasion of Ukraine on 24 February 2022, Belarusian railway workers posted a message on their Telegram-channel @belzhd_live in which they reported the arrival in Belarus of trains carrying military equipment and personnel of the Russian Federation Armed Forces for the joint Belarus-Russian exercise Allied Resolve. 'The total number of trains that will arrive in Belarus – 200 military echelons – is an outrageous figure', the message read, also noting that during the earlier joint strategic exercise ZAPAD 2021 'only 29 military echelons' had been sent to Belarus.[1] The message was preceded by what has been called the largest Russian military deployment in Belarus since the end of the Cold War. According to press reports, by the beginning of February 2022, 30,000 Russian troops had arrived in Belarus for joint military exercises.[2] Some of the units deployed to Belarus came from places as far as Lake Baikal in Russia's Eastern Military District.[3]

Then, on Monday 24 January 2022, a group calling itself the Belarusian Cyber Partisans posted messages on their social media channels Twitter (13,500 followers) and Telegram (63,000 followers), claiming to have encrypted the Belarus Railways (BR) servers, workstations and databases.[4] According to the Cyber Partisans, the direct aim of this operation was to disrupt the activities of BR as a sign of protest because President Aleksandr Grigorjevitsj Lukashenko of Belarus had allowed 'occupying troops to enter our land'.[5] The Belarusian Cyber Partisans have found themselves at loggerheads with the Belarus regime since August 2020 when, after fraudulent presidential elections, Lukashenko refused to cede power to the opposition and crushed a popular revolt by using harsh measures towards protesters, exiling opposition leaders and detaining thousands of opposition members.

Operations in cyberspace by non-state actors against state actors are not a new phenomenon.[6] For more than a decade the hacker collective Anonymous, an important benchmark for these type of action, has not hesitated to attack governments and firms in cyberspace for alleged misdoings.[7] The Anonymous 'group' has claimed responsibility for several website defacements, information leaks and distributed denial of service (DDOS) attacks.[8]

In the analysis of these operations frameworks can be used such as the '(unified) cyber kill chain'.[9] This operational framework focusses heavily on the techniques, vectors, vulnerabilities and exploits used to seek effects with the cyber operations. These frameworks, however, offer little insight into motives and focus primarily on so-called 'hacking' or 'hard cyber operations'. But is this label appropriate for the activities of the Belarusian Cyber Partisans or are other, more precise, definitions possible?

A photo made available by the Belarusian government shows Russian military vehicles arrive for the joint military exercise 'Allied Resolve' in Belarus, 18 January 2022. The Belarusian Cyber Partisans claimed to have encrypted the Belarus Railways servers, aiming to disrupt such transports

PHOTO ANP/EPA/BELARUS DEFENCE MINISTRY

* Major Peter Schrijver is PhD-researcher at the Netherlands Defence Academy (NLDA). Brigadier-general Paul Ducheine is Professor of Cyber Warfare at the NLDA. This article is based on a Master Military Strategic Studies research paper.

1 @belzhd_live (Belarusian railway workers, Telegram channel), 'Live. Сообщество Железнодорожников Беларуси'. https://t.me/belzhd_live/1257.

2 Pavel Polityuk and Sabine Siebold, 'NATO Says Russia to Have 30,000 Troops on Drills in Belarus, North of Ukraine', *Reuters*, 3 February 2022.

3 Michael Sheldon, 'Russian Military Equipment Spotted in Belarus as Tensions Heighten with Ukraine', *@DFRLab*, 18 January 2022.

4 @cpartisans_bot (Telegram channel Belarusian Cyber Partisans) 'Кибер-Партизаны'. https://t.me/cpartisans/625.

5 'Why the Belarus Railways Hack Marks a First for Ransomware', *Wired.com*, 25 January 2022.

6 R.J. Buchan, Cyberspace, 'Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law*, 21 (3) (2016) pp.429-453.

7 Paulo Shakarian, Jana Shakarian and Andrew Ruef hakarian, *Introduction to Cyber-Warfare. A Multidisciplinary Approach* (London, Syngress, 2013) p.79.

8 Johan Sigholm, 'Non-State Actors in Cyberspace Operations', *Journal of Military Studies*, 4 (1) (2013) 3.

9 See i.a. Paul Pols, *The Unified Kill Chain. Raising resilience against advanced cyber attacks through threat modeling*: www.unifiedkillchain.com.

Belarusian Cyber Partisans: resistance in cyberspace

The Belarusian Cyber Partisans hacker collective emerged in 2020 in response to the controversial presidential elections and following crackdown on civil liberties in Belarus. The group consists of Belarusian activists, hackers and IT professionals who use their skills to challenge the regime of President Aleksandr Lukashenko and support the pro-democracy movement.

The cyber partisans rose to prominence in August 2020 when they launched a massive cyber-attack against government propaganda websites and leaked sensitive information about the country's security services. The group has claimed responsibility for several high-profile cyber-attacks, including in 2022 on systems of Belarusian Railways to disrupt incoming Russian military transports.

The group operates in secrecy, using an enhanced variant of the messaging app Telegram to evade detection and retaliation by authorities. Belarusian cyber activism has received widespread support from the international community and has been praised for its efforts to promote human rights and democracy in Belarus. However, their actions also angered the Belarusian government, which called them 'terrorists' and threatened them with severe punishment if caught. Overall, the Cyber Partisans represent a form of activism that uses technology and digital tools to challenge authoritarian regimes.

Sources: Andrea Peterson, 'Cyber Partisans hacktivists claim credit for cyberattack on Belarusian Railways', *The Record*, 24 January 2022; Andrew Roth, ''Cyberpartisans' hack Belarusian railway to disrupt Russian buildup', *The Guardian*, 25 January 2022; Dalton Bennett and Robyn Dixon, 'How Belarus's 'Cyber Partisans' exposed secrets of Lukashenko's crackdowns', *The Washington Post*, 15 September 2021

Aim and Relevance

This article firstly aims to enhance insight into the activities of the Belarusian opposition in cyberspace. This contributes to the understanding of the dynamics in the information environment in Belarus, which borders on Lithuania where a Netherlands company within the NATO enhanced Forward Presence (eFP) mission is stationed. In particular, it will shed light on the context of the cyberspace activities against the Belarus regime since 2020. Although the actions of the Belarusian cyber group succeed in increasing media attention, little is known about the background of this group, which aligns itself with the Belarusian opposition leadership.[10]

Secondly, apart from gaining more operational insight into the modus operandi of the various operations described to (or claimed by) the Cyber Partisans, this article also aims to offer more conceptual clarity on effects sought by these non-state groups, and thereby on how the Belarus Cyber Partisans should be labelled.

Structure

This article limits itself to examining the context of the activities of the Belarusian Cyber Partisans (BCP) in cyberspace against the Belarus regime during and after 2020. It will therefore offer a conceptual framework for influence operations first. It will then describe the Cyber Partisans activities against the Belarus regime. Subsequently, the various activities will be analysed using the model presented.

Conceptual framework

Traditionally, cyber operations are divided into the broad categories of hard and soft cyber power.[11] According to Joseph S. Nye, an example of hard power in cyberspace is when states or non-state actors organise a DDOS-attack to paralyse the internet system of an opponent.[12] An example of soft power in the cyber domain is persuading a group of programmers to adhere to a new software standard.[13] In that sense the Stuxnet Operation, which targeted the centrifuges of Iran's uranium enrichment plants, using

10 'Belarusian Cyber-Partisans Want to Overthrow the Regime through Hacking', *Deutsche Welle*, 3 September 2021.

11 Joseph Nye Jr, *Cyber Power* (Cambridge, Harvard Kennedy School/Belfer Center for Science and International Affairs, 2010) p.6.

12 Idem, p.5.

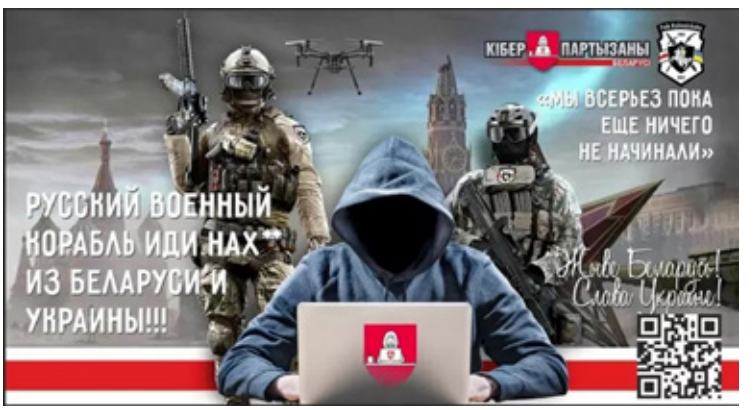
13 Ibidem.

stealthy software to disrupt industrial control systems would be classed as hard cyber power and the interference with the US elections in 2016 through influence operations in cyberspace as soft cyber power.[14]
Sean Cordey of the Swiss ETH Center for Security Studies (CSS) approaches cyber operations from the generic angle of influence operations, which were already a characteristic of pre-conflict and conflict phases long before there even was a mention of cyber operations and/or cyberspace.[15] The ETH CSS definition of cyber influence operations is as follows: 'the term cyber influence operations (CIOs) refers to illegitimate (sometimes illegal) activities that are run in cyberspace, leverage the distributed vulnerabilities of cyberspace, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes'.[16]

Based on the means and ways applied his definition is then subdivided into two separate spheres.[17]
First, Cyber-enabled Technical Influence Operations (CeTIO) disturb 'cyberspace through intrusive means to gain unauthorized access to networks and systems in order to destroy, change, steal or inject information with the intention of influencing attitudes, behaviors, or decisions of target audiences'.[18] Basically, this definition refers to the hacking of computer systems.

Secondly, Cordey then goes on to explain Cyber-enabled Social Influence Operations (CeSIO), which 'target and attack the semantic layer of cyberspace (i.e. information content) through a wide variety of tools and techniques in order to support and amplify various political, diplomatic, economic, and military pressures'.[19] This definition is tied to influence operations, for example the distribution of disinformation via social media channels.

According to these definitions, DDOS-attacks or hacking into IT-systems – which are traditionally labelled hard cyber operations – belong to the sphere of cyber-enabled influence operations. The ETH CSS argues these DDOS-attacks on



Belarusian Cyber Partisans: 'Russian war machine, leave Belarus and Ukraine. We have not even started'

institutions in Estonia in 2007 had the ultimate goal of undermining trust in the Estonian government and should therefore not be called hard cyber operations but be considered as Cyber-enabled Technical Influence Operations.[20] Actions which sow and amplify disinformation via cyberspace with the goal of undermining trust in institutions are not soft cyber operations but Cyber-enabled Social Influence Operations.[21]

Hence, the ETH CSS postulates that cyber operations aiming to influence persons, communities and even regions or countries should thus be labelled as cyber-enabled influence operations. The modus operandi used to influence will, subsequently, be further categorised as either technical (e.g. hacking) or social (e.g. spread of disinformation on Twitter).

14 Petere Pijpers and P.A.L. Ducheine, 'Influence Operations in Cyberspace – How They Really Work' (September 24, 2020), Amsterdam Center for International Law No. 2020-31, Available at SSRN: https://ssrn.com/abstract=3698642 or http://dx.doi.org/10.2139/ssrn.3698642.
15 Sean Cordey, 'Cyber Influence Operations: An Overview and Comparative Analysis', (ETH Zürich, October 2019) p.6.
16 Cordey, p.11.
17 Which is similar to the Russian division between information technological warfare and information psychological warfare, see: Keir Giles, *Handbook of Russian Information Warfare*, *NATO Defence College* 9, no. November (2016): pp.1-90, 9.
18 Cordey, p.15.
19 Cordey, p.16.
20 Cordey, p.15.
21 Cordey, p.17.

1. Preparation/ Reconnaissance	2. Execution cyber-related activities		3. Exploitation/ Objective
	Cyber-enabled Technical Influence Operations	**Cyber-enabled Social Influence Operations**	
• Political intent • Strategic narrative • Identify fissures • Map and segment audience • Framing • Creation (websites, content)	• DDos/DOS • Defacement • Hacks	• Cognitive hacking • Social hacking • Disinformation • Doxing • Forging & leaking • Potemkin villages • Deceptive identities • Bots/botnets • Trolling & flaming • Humor & memes	• Disrupt activities – sense of insecurity • Control/reinforce/redirect narrative • Undermine trust in institutions/media/allies • Demoralise/encourage • Sow division/polarise • Discredit/support individuals

Figure 1 Framework derived from Pijpers, ETH CSS Zürich and CSET, for the purpose of identifying different types of cyber-enabled influence operations (IO)

To bring operational and conceptual clarity in the activities of the Belarusian Cyber Partisans in cyberspace against the Belarus regime as of 2020, a combination of frameworks/analytical models is used.[22, 23, 24] A possible model could be figure 1 shown above.

Activities in cyberspace against the Belarus Regime since 2020

This section gives an overview of the cyberspace activities against the Belarus Regime since 2020. It will give a chronological summary starting with activities executed shortly after the fraudulent presidential elections in August 2020 and ending with the claim of the Belarusian Cyber Partisans to infringe the systems of the Russian internet and media regulator Roskomnadzor in November 2022. In 2021, Operation Heat was the most notable example of the capabilities of the Cyber Partisans. However, they had already given hints of their expertise as of September 2020, with the defacement of government websites[25] and the interruption of internet news programmes by state TV channels *Belarus 1* and *ONT* by showing clips of police brutality instead of regime-censored news.[26]

Summer of 2020: fraudulent elections followed by a harsh crackdown

After the elections in August 2020, despite almost openly fraudulent actions, Lukashenko began his sixth term as President of Belarus since 1994. Though elections had been rigged before and despite the regime's effort before the elections to crack down on the opposition by jailing its leaders and banning their candidacies, this time it was different. Not least since Svyatlana Tsikhanouskaya – the wife of candidate Syarhei Tsikhanousk – stepped in. Tsikhanousk was a well-known video blogger who had been imprisoned after leading an enormously popular – though not very subtle – campaign called 'Stop the Cockroach'.[27] Along with Tsikhanouskaya, the wives of other jailed politicians and campaigners united in one opposition front, which, according to exit poll

22 Pijpers, 'Influence Operations in Cyberspace'.
23 Cordey, 'Cyber Influence Operations: An Overview and Comparative Analysis'.
24 Katerina Sedova et al, 'AI and the Future of Disinformation Campaigns' (Center for Security and Emerging Technology, December 2021) p.2.
25 'Lukashenka's Regime Confused about Belarusian Cyber-Partisans' Activity', *@DFRLab*, 1 October 2020.
26 Belarus Free Theatre, 'Cyber Partisans in #Belarus Hacked the Websites of the Main State TV Channels, Instead of the Government Propaganda They Showed the Beatings and Arrests of Protestors in the Live TV Section. See: https://T.Co/GMqpvrKESR'.
27 'Stop the cockroach': protests rattle Belarus President Lukashenko before election', *Reuters*, 2 June 2020.

Riot police clash with protesters in Minsk, capital of Belarus, after President Lukashenko denied to step down after fraudulent elections in 2020 *Photo Picture Alliance/Anadolu Agency*

data collected by various online platforms, would presumably have won the elections.[28] From that moment on mass protests began to break out in the capital Minsk and in other Belarusian cities. The regime increasingly resorted to excessive violence and mass detentions to crack down on the peaceful manifestations. The regime imprisoned more than 30,000 persons, mostly on trivial charges such as displaying symbols related to the opposition, presence at a demonstration or even a single social media post that was critical of the regime.[29] These events caused opposition leaders such as Tsikhanouskaya to go into exile in neighbouring Poland and Baltic states Lithuania and Latvia. Progressively, the security apparatus succeeded in suppressing open rebellion against the regime of President Lukashenko and in the winter of 2020/2021, mass protests on the streets of the cities in Belarus slowly stopped.[30]

Operation Heat

However, this was not the end of the resistance against Lukashenko's regime. In a series of hacks in the summer of 2021 the Belarusian Cyber Partisans, which reportedly consists of 10 to 15 Belarus IT experts,[31] managed to penetrate deeply into government databases.[32] Contrary to what a casual observer might think, Belarusian IT-expertise is traditionally one of the trademarks of the Belarusian economy. Already during the era of the Soviet Union, Belarus developed into a hub of the then emerging IT sector.[33] Belarusian IT skills are still sought after on the global market.[34]

28 'It's outrageous: Belarus election result sparks night of defiance and violence', *The Guardian,* 10 August 2020.

29 Human Rights Watch, 'Belarus'. See: https://www.hrw.org/europe/central-asia/belarus.

30 Deutsche Welle, 'Belarus'. See: https://www.dw.com/en/belarus/t-38384925.

31 'Details Emerge on Hack of Belarusian Railways and the Group behind It. The hackers posted 'proof' of their hacks, and researchers have started to dig in', *Cyberscoop*, 26 January 2022.

32 Andrei Soshnikov et al., 'Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data', *Current Time*, 4 August 2021.

33 Foreign Policy Research Institute, 'How Belarus' Soviet Past Led to its Modern-Day IT Success', See: https://www.fpri.org/article/2020/12/how-belarus-soviet-past-led-to-its-modern-day-it-success/.

34 Rest of World, 'The tech workers exiled from Europe's last dictatorship', See: https://restofworld.org/2023/belarus-tech-exile-lukashenko/.

The BCP managed to retrieve 5.3 million recordings of tapped telephone conversations from databases of the Belarus Interior Ministry

This high level of home grown IT-knowledge in Belarus may have helped the BCP in the summer of 2021, when the group managed to retrieve 5.3 million recordings of tapped telephone conversations from databases of the Belarus Interior Ministry.[35] Dimitri Alperovitch, an American cyber security specialist posted a message on Twitter: 'This is as comprehensive of a hack of a state as one can imagine.'[36] The American Center for European Policy Analysis (CEPA) qualified it as 'the most successful cyber-attack in the history of Belarus, involving entry to the regime's most secret and sensitive data vaults', describing the scale of the hack as unprecedented.[37]

The Cyber Partisans released a phone call from their trove which had been recorded just after the elections in August 2020, in which a subordinate, asking how to handle a group of peaceful protestors – mainly women in Minsk – received a reply from a colonel of the Interior Ministry's Minsk department of the Public Security Police that he should arrest them and beat them.[38]

The Cyber Partisans published the call on multiple (social) media channels, exposing the ruthless tendencies of those loyal to the regime. Apart from police brutality, other released phone recordings showed similar behaviour from officers responsible for security in Belarusian cities, including one officer in Brest who stated that 'the more of his 500 detainees […] sent to hospital after rough treatment, the better'. In August 2020 the *BBC* already reported on police firing live rounds at protestors in Brest.[39] To this day, the BCP regularly leak recorded phone calls between security and/or government personnel from the mid-2021 hack.[40]

Operation Scorching Heat 2022

The next operation through which BCP managed to attract attention worldwide, was a hack into the IT systems of Belarusian Railways. On 24 January 2022, the group posted the following message on several social media channels: 'At the command of the terrorist Lukashenko #Belarusian Railway allows the occupying troops to enter our land. We encrypted some of BR's servers, databases and workstations to disrupt its operations'.[41] The group stressed that in order to prevent dangerous railway conditions, BR's safety systems were not affected by the attack. The group claimed that it would be willing to release its grip on the BR systems when its demands, namely the release of fifty political prisoners and a halt to the influx of Russian troops, had been met.[42] Just before the hack, the BR railway workers union had placed a message on its Telegram channel stating that BR was set to receive record numbers of trains in Belarus carrying Russian military equipment as part of the Russian-Belarus joint exercise Allied Resolve.[43]

The visible result of the hack by the BCP, coined Operation Scorching Heat, was the interruption of the electronic ticket system for passengers.[44] The group itself claimed that it was easy to access the BR network due to obsolete IT

35 Dalton Bennett and Robyn Dixon, 'How Belarus's 'Cyber Partisans' Exposed Secrets of Lukashenko's Crackdowns', *The Washington Post*, 15 September 2021.

36 Dmitri Alperovitch, 'This Is as Comprehensive of a Hack of a State as One Can Imagine', *Twitter*, 2 September 2021.

37 CEPA, 'Lukashenka's Secrets: Not So Secret Anymore', See: https://cepa.org/article/lukashenkas-secrets-not-so-secret-anymore/.

38 You Tube channel Cyber Partisans, See https://www.youtube.com/watch?v=fPsiabcdiPU.

39 BBC News, 'Belarus election: Police use live fire on protesters in Brest', See: https://www.bbc.com/news/world-europe-53748748.

40 Bennett and Dixon, 'How Belarus's "Cyber Partisans" Exposed Secrets of Lukashenko's Crackdowns', *The Washington Post*, 15 September 2021.

41 Greenberg, 'Why the Belarus Railways Hack Marks a First for Ransomware'.

42 ZD NET/tech, 'Belarusian activists launch ransomware attack in protest of dictatorship, Russian troop surge', See: https://www.zdnet.com/article/belarusian-activists-launch-cyberattack-against-railway-in-protest-of-dictatorship-russian-troop-surge/.

43 @belzhd_live (Belarusian railway workers, Telegram channel), 'Live. Сообщество Железнодорожников Беларуси 🤍'.

44 Dan Goodin, 'Hactivists Say They Hacked Belarus Rail System to Stop Russian Military Buildup', Ars Technica, 24 January 2021.

PHOTO ANP/ANATOLIY ZHDANOV/KOMMERSANT/SIPA USA

In November 2022 the BCP said they had infringed the systems of Roskomnadzor, responsible for monitoring online content in Russia, claiming to have obtained a large amount of data

infrastructure and published several internal BR documents as proof of their breaching success.[45] The Cyber Partisans indicated that they had gained access to the BR systems because they were aware that BR personnel were using illegal software, which needs so-called 'cracks' or 'crack software' in order to run. These 'cracks' can be downloaded from shady websites.[46] Access to the BR network may have been gained after a BR employee unwittingly downloaded a possibly tailored piece of 'crack software' from such a website via a computer connected to the BR network, which enabled the installation of malware.[47]

Several private US based cyber security agencies commented on the credibility of the Scorching Heat hack. SentinelOne stated that it was 'unable to confirm the ransomware attack but that the images provided appeared to confirm someone gained privileged access to Belarus Railway's network'.[48] The phrase 'images provided' refers to several screenshots of documents from BR databases captured by the Cyber Partisans. These screenshots, published on Twitter, showed recent documentation of communications between BR and Russian

45 James Beardsworth, ''Hacktivist' Cyber Disruption Could Spread to Russia, Experts Believe', *The Moscow Times*, 1 February 2022.

46 Belarusian Cyber Partisans, 'Screenshots Taken during a #ScorchingHeat Cyberattack on the #belarus Railroad Reveal That Employees Frequently Used Pirated Software. Do You Think It's Connected to How They Got Hacked? 🤔🤔🤔 Https://T.Co/De2R6W4Jt3'.

47 Hypothesis by authors after conversation with forensic cyber expert (NLD Army reservist).

48 Goodin, 'Hacktivists Say They Hacked Belarus Rail System to Stop Russian Military Buildup'.

railway IT personnel, and an internal BR document requesting that outdated workstations running on Windows XP be replaced.[49]

In the course of 2022 the BCP continued their campaign to put pressure on the Belarusian regime. The BCP gained access to passport data of all Belarusian citizens. Although these data were not extensively released to the public, interested parties were offered non-fungible tokens (NFT) of President Lukanshenko's passport as a publicity stunt and fundraising campaign to continue actions against the government.[50] The BCP follow a pattern of not only breaching into government databases but, subsequently, the organisation also seeks ways to maximise publicity around their hacks by providing journalists and research collectives, e.g. Bellingcat access to acquired material.[51] In November 2022 the BCP once again were able to hit international headlines after they had infringed the systems of Roskomnadzor, responsible for monitoring online content in the Russian Federation.[52] BCP claimed to have obtained large amount of data, including emails and other documents, totalling over two terabytes.[53] It was also reported that the hacktivist group encrypted certain workstations and damaged the domain controller. Roskomnadzor acknowledged the breach but attributed it to the exploitation of a previously unknown vulnerability.[54]

49 'Details Emerge on Hack of Belarusian Railways and the Group behind It'.
50 A.J. Vicens, 'Belarusian Hacktivists Try NFTs to Support Antigovernment Campaign', *Cyberscoop*, 31 August 2022.
51 Christo Grozev [@christogrozev], 'We First Noticed Her Thanks to a Super Useful Database Shared with Us by @cpartisans: The Border Crossing Records of Belarus. We Knew the Passport Ranges of GRU and FSB Spies, so We Decided to Search in That Data-Set by Partial Matches, Leaving the Last 3 Digits out as Wildcards.'
52 Daryna Antoniuk, 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator', *The Record*, 22 November 2022.
53 Gintaras Radauskas, 'Russian Censors Suffer Another Massive Hack', *Cybernews*, 21 November 2022.
54 Antoniuk, 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator'.
55 ' Details Emerge on Hack of Belarusian Railways and the Group behind It'.
56 Unit, 'A Web Interface for the GDELT Project'. Source: https://www.gdeltproject.org/.
57 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator'.
58 Antoniuk, 'Hacktivist Group Shares Details Related to Belarusian Railways Hack'.
59 Soshnikov et al., 'Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data'.
60 Patrick Howell O'Neill, 'Hackers Are Trying to Topple Belarus's Dictator, with Help from the Inside', *MIT Technology Review*, 26 August 2021.

Failure and success of Operation Scorching Heat

With regard to the Scorching Heat attack of January 2022 and later attacks that year, it must be assessed that the original demands of the Belarusian Cyber Partisans were not met: it appears that the regime did not release political prisoners and did not halt the influx of Russian military and personnel into Belarus. In fact, in February 2022 Russian troops located on Belarusian territory were tasked to take the Ukrainian capital Kyiv. In this respect, the ransomware attack on BR was of little or marginal effect, besides the disturbance of electronic ticketing, the capture of internal BR documentation and the claimed encryption of servers, workstations and databases. Although this caused considerable damage to BR daily operations, the BR activities seemingly proceeded to continue as usual.[55] Thus, the operation could be considered as a minor success. However, amplified by the worldwide interest being paid to the Russian military build-up around Ukraine during the winter of 2021/2022, the January hack by the Cyber Partisans into the BR network gained worldwide media attention. Around the time of the hack (24-25 January 2022), approximately 6,000 articles appeared in press and media in which the BCP were mentioned.[56] The hacking of the Belarusian passport data records and the Russian internet regulator Roskomnadzor also received attention in global media outlets.[57] The earlier data hack (Operation Heat) into the Belarus Interior Ministry in mid-2021, which was of a much larger scale, attracted less attention in the international press.

Exposing the regime

Worldwide media attention set aside, the Belarusian Cyber Partisans have repeatedly stated that the overall goal of their actions is to expose the Belarusian regime[58] and take away the cloak of anonymity of government employees responsible for human rights abuses of Belarusian citizens.[59] The BCP explained that they wanted 'to stop the violence and repression from the terroristic regime in Belarus and to bring the country back to democratic principles and rule of law'.[60] To do so, the data, including details of security personnel which the Cyber

PHOTO PICTURE ALLIANCE/DURSUN AYDEMIR/ANADOLU AGENCY

Svyatlana Tsikhanouskaya speaks during the 2020 Sakharov Award Ceremony in Brussels: the European Parliamant considers Tsikhanouskaya and other opposition leaders to be the true ligitimate representatives of Belarus

Partisans collected during Operation Heat in 2021, are also shared with other activists. On the Telegram channel 'Black Book of Belarus' and the website Blackbook.org, data are published that identify members of the Belarus security services. Yanina Sazanovich, an editor of the Telegram channel, argues: 'In this war, we don't have any weapons. We have truth and 'de-anonymization' and this is our power and we will use it'.[61] The government of Belarus rarely comments on the attacks carried out by the BCP or pretends to be unaware of them.[62] Pro-Lukashenko Telegram channels Belaruskaya Kuhnya and #InfoSpecNaz Belarusii have branded the Cyber Partisans as 'employees of NATO cyber centers carrying out information and psychological attacks'.[63]

The aim of the Belarusian Cyber Partisans is to stop the violence and 'to bring the country back to democratic principles and rule of law'.[64] The BCP influence activities do not solely affect the cognitive dimension. In the physical dimension, real-world information (personal data) is provided on the home addresses of regime members. In the virtual dimension, hack operations result in the disturbance of IT systems such as the Belarus Railways ticketing system or the defacement of websites. Physical and virtual activities add up to effects in the cognitive dimension, including activities outside Belarus, such as the promotion of anti-regime protest in European capitals in the physical dimension.

The combined activities in all three dimensions are designed to undermine the resilience of the Belarus regime with the aim of ending it, which is one of the stated goals of the BCP.

61 'How Belarus's 'Cyber Partisans' Exposed Secrets of Lukashenko's Crackdowns'.
62 'Lukashenka's Regime Confused about Belarusian Cyber-Partisans' Activity'.
63 @DFRLab.
64 O'Neill, 'Hackers Are Trying to Topple Belarus's Dictator, with Help from the Inside'.

Belarusian Railway was once again the target of a hack in an attempt to slow down the transfer of occupying forces and give the Ukrainians more time to repel the attack

Defining the operations of the Belarusian Cyber Partisans

In this section the BCP operations of the Cyber Partisans are analysed against the conceptual framework used for the analysis of cyber-enabled influence operations, which encompass three consecutive phases of preparation/reconnaissance, execution of cyber-related activities and exploitation. The model (figure 1) offers an opportunity to assess whether the operations of the Belarusian group fit in the ETH CSS categorisation of Cyber-enabled Technical or Social Influence Operations.

Outcome

Nearly all activities of the Belarusian Cyber Partisans can be placed in a framework (figure 2) defining cyber-enabled influence operations. As such, the specific input provided by ETH CSS is helpful in categorising activities which involve the influencing of audiences and the input increases understanding of (non-state) activities in cyberspace. The analysis also shows that while a conceptual categorisation of cyber-activities can be made, to gain cognitive effect in or via cyberspace both operational avenues (technical and social) to influence are used. Hence, actors in cyberspace – including BCP – should not upfront be labelled as hard- or soft cyber operators.

Though the ETH CSS definition of cyber-enabled influence operations is helpful, there is also a flaw with this type of labelling as 'the term cyber influence operations (CIOs) refers to illegitimate (sometimes illegal) activities' only.[65] It is outside the scope of this article to determine when influence operations are unlawful.[66] However, while the Belarusian regime regards the activities undertaken by the Belarus Cyber Partisans as illegitimate, Poland and Lithuania harbouring sizeable contingents of Belarusian exiles, and the European Parliament, all consider the Belarusian opposition to be the true (legitimate) representatives of Belarus.[67]
In sum, conceptual frameworks are useful in assessing the nature of the operations in cyberspace, but some prudence must be taken since the frames will not be universally applicable. ETH CSS' definition, for instance, places the emphasis on rogue actors using cyber-enabled influence operations, hence, lacks an inclusive approach.

Conclusion and epilogue

In this article the activities of the Belarusian Cyber Partisans against Lukashenko's regime during and after 2020 were addressed offering operational insights. The organisation presents itself as a non-state actor which supports the Belarus opposition by executing cyber operations aimed at undermining the Belarus regime. To provide conceptual clarity for their operations, a framework for the appraisal of cyber-enabled influence operations was used, based on work of scholars such as Pijpers and of the research institutes CSET and ETH CSS.

The article focused on the context of the activities in cyberspace. Cyber operations by the BCP are meant to influence an actor or actors, in this case primarily the Belarusian regime (undermine its resilience), but also the Belarusian population itself as well as foreign governments and populations. This aim or purpose – to influence audiences – is the main criterion for labelling the activities. Subsequently subdividing these by operational means and ways (technical or social) into cyber-enabled social and technical

65 See footnote 22.

66 On this topic see e.g. Peter B.M.J. Pijpers, *Influence Operations in Cyberspace. On the Applicability of Public International Law during Influence Operations in a Situation Below the Threshold of the Use of Force* (Thesis, University of Amsterdam, 2021).

67 'Lithuania Gives Belarusian Opposition Official Status', *Radio Free Europe*, 5 July 2021.

1. Preparation/ Reconnaissance	2. Execution cyber-related activities		3. Exploitation/ Objective
Intent: Bring Belarus to democracy and return rule of law	**Cyber-enabled Technical IO** Website defacement of Belarus TV-stations	**Cyber-enabled Social IO** Doxing of government personnel and security officers	Disrupt activities – sense of government not in control
Narrative(s): Lukashenko's regime is undemocratic	Content replacement in government-related websites	Leaking details from official sensitive documentation	Reinforce narrative about regime being undemocratic
'We have no weapons'	Hack into sensitive databases of the Interior Ministry	Social engineering (making use of inside knowledge /weaknesses	Russian troop movements in Belarus are illegal
Stop repression by regime	Access to footage of surveillance cameras	Humor & memes	Undermine trust in infrastructure
Release political prisoners	Hack into license plate database service		Demoralise security personnel government
Russian troops in Belarus are not welcome			Deanonymisation (actions of regime personnel are noted and recorded)
Regime is negligent of infrastructure ('hacking into IT-systems is easy')			Discredit government-related individuals

Figure 2 Activities of the Belarusian Cyber Partisans outlined in a framework to identify different types of cyber-enabled influence operations

influence operations is helpful in understanding the true nature of these actions, instead of using the more generic terminology of hard and soft cyber operations.

Given the current situation in which the Belarusian regime is inclined to strengthen its ties with the Russian Federation, Operation Heat and Operation Scorching Heat proved not to be the final activities of the BCP for the world to notice. On 24 February 2022 the group announced on its social media channels that it would contribute to the defence of Ukraine.[68] Since then, the BCP reached out to cooperate with groups such as the IT Army of Ukraine.[69] Shortly after Russia's invasion the Cyber Partisans stated that the state company Belarusian Railways was once again the target of a hack in an attempt to 'slow down the transfer of occupying forces and give the Ukrainians more time to repel the attack'.[70] As such, the BCP moved from influence operations seeking cognitive effects to physical impact operations too. ■

68 Belarusian Cyber Partisans, '#Ukrainians and #belarusians Have a Common Enemy: Putin, Kremlin, the Imperial Regime. We Call on Everyone to Share This Info and Contact Us If Any Volunteers Want to Join Our Group. Please Support, Many Resources Are Still Needed: Bc1qvf5jeswp0tu9s7kuf5uzjges49gnf0637asa8l'.

69 Stefan Soesanto, 'The IT Army of Ukraine. Structure, Tasking, and Eco-System' (ETH Zürich, June 2022) p.27.

70 'Belarusian hackers launch another attack, adding to chaotic hacktivist activity around Ukraine', *Cyberscoop*, 28 February 2022.