Navigating the Cyber Front: Belarus' State Control and Emerging Cyber Threats

Darius Štitilis[1], Marius Laurinaitis[1], Inga Malinauskaitė-van de Castel[1] and Matthew Warren[2]
[1]Mykolas Romeris University, Vilnius, Lithuania
[2]RMIT Univeristy, Melbourne, Australia

stitilis@mruni.eu
laurinaitis@mruni.eu
inga.malinauskaite@mruni.eu
matthew.warren2@rmit.edu.au

Abstract: This paper provides a comprehensive overview of the cyber landscape in Belarus, with a focus on the Belarus government's use of cyber activities from an offensive and defensive context, the emergence of opposition cyber activities, and the broader implications for cybersecurity and legal compliance. In the course of the research, researchers try to assess Belarus as a source of cyber-threats, both domestically and to neighbouring states (especially those supporting Ukraine). The first section of the paper outlines the Belarusian government's engagement in cybercrimes against its citizens, especially under President Lukashenko's regime, highlighting extensive online surveillance, repression, and the escalation of these activities following the 2020 presidential elections. In this political context, Belarus is also examined as a country initiating and/or contributing to Information Warfare activities, which are mainly directed at western countries. The second section of the paper delves into Belarus's cybersecurity legal framework, examining various national strategies and concepts, the absence of a formal cybersecurity strategy, and the focus on 'information security' as part of national security. The third section presents case studies of cyber activities in Belarus, contrasting government-backed hacking efforts with those of opposition groups like the Belarus Cyber Partisans. It explores the Partisans' attacks on state infrastructure and information leaks as a form of protest against the government, and the pro-government hackers' disinformation / information campaigns website defacements, and data breaches, particularly targeting Ukraine. This section highlights the evolving nature of cyber conflict in Belarus, where both government and opposition forces use cyber tools for political ends, reflecting broader geopolitical tensions in the region. This part of the report compares the Belarusian pro-government hacktivist and Cyber Partisans groups, their activities and manifestations within the country (inside), as well as the cyber threats they pose to foreign countries. The article attempts to answer the question of what kind of threat Belarus as a country poses in the context of cybersecurity, hybrid-cyber threats. This country is often included in Russian hybrid-cyber threats strategies, Belarus entities also work with Russian and sometimes Chinese groups in undertaking cyber activities against other countries.

Keywords: Cyber Security, Belarus, Hackers, Fake News, Hybrid Threats and State Based Attacks.

1. Introduction

Belarus, located in Eastern Europe, is a landlocked country bordered by Russia to the northeast, Ukraine to the south, Poland to the west, and Lithuania and Latvia to the northwest. Covering an area of approximately 207,600 square kilometres. As of 2023, Belarus has an estimated population of around 9.4 million people. Belarusian and Russian is the official language, reflecting the country's deep historical and cultural ties with Russia.

Belarus maintains close geopolitical ties with Russia, often described as a key ally in Eastern Europe, sharing strong political, economic, and military connections, including a formal union state agreement with Russia. This relationship significantly influences Belarus' foreign policy and regional dynamics, particularly in its stance towards NATO and the European Union.

Belarus is closely aligned with Russia, has emerged as a notable source of hybrid threats within Eastern Europe, particularly in the cyber domain. Hybrid threats from Belarus to Eastern Europe involve a combination of conventional and non-conventional tactics designed to undermine and destabilize nations[1]. Belarus is aligned more closely with Russian strategic goals, Belarus will likely develop more severe hybrid threats to its European neighbourhood (Rusinaite V, 2021).

[1] Disinformation campaigns, cyber attacks, economic pressures, military posturing, political interference, etc.

2. Belarus Cyber Background

The Belarusian authorities have consistently committed many crimes including cybercrimes against its own citizens, especially in the context of the regime of President Alexander Lukashenko. Since Lukashenko became President in 1994, he has established a control mechanism involving extensive online surveillance and repression of citizens, particularly those who oppose the regime (O'Neill, 2021). The situation has escalated following the disputed presidential elections in August 2020, which led to widespread protests and opposition to Lukashenko's rule. The government's response to these protests has included a violent crackdown on peaceful dissent, underlining the regime's oppressive tactics against its own citizens.

In the first decade of the 21st century, internet censorship in Belarus developed as an effective tool of control against political opponents. State-sponsored DDoS attacks against civil society have become an internal crisis that threatens not only freedom of expression in Belarus, but also the integrity of internet resources across Europe. The ongoing cyber conflict between state and non-state actors in Belarus is analogous to the cyber struggle between the Russian government and its internal enemies. On 9 September 2001, at 12.00, Belarusian web developers clashed with the authorities for the first time – on the day of the presidential elections. The national telecommunications company Beltelecom, the monopoly service provider in this area, deliberately blocked access to several popular political websites. The next day internet censorship started. From a technical point of view, such blocking of information is not a difficult task for a telecommunications monopoly and can be directed by the government as needed (Czosseck, Geers, 2009).

It must be pointed out that there was no legal basis for internet censorship within Belarus. Such censorship was in direct violation of the Belarusian Constitution (Disrupting systems is a crime under Belarusian law (Criminal code of Belarus, 1999)). The official explanation given by the Belarusian Ministry of Communications and the government controlled telecommunications company was that too many users were trying to access the websites in question at the same time, which led to the service being blocked.

Another example of such state cyber-censorship was the blocking of the popular Belarusian website Charter 97 (Pavlyuchenko, 2009). The Belarusian Ministry of Information published the official reasons for its decision to restrict access to the charter97.org website, claiming that the site disseminates information that could harm Belarus' national interests, as well as violating the Law on Mass Events and publishing material that has been identified as extremist. The basis for blocking the website was Article 38 of the "Law on Media", which has been repeatedly criticised by human rights activists as discriminatory and undemocratic.

The authorities in Belarus have consistently tried to suppress political criticism online internally and externally to Belarus. There is no legal basis for internet censorship in Belarus, in particular in relation to being critical of official online information sources. Only one case of official censorship can be found (officially acknowledged by the Belarusian government): in 2005, a pornography website run by a Russian citizen was blocked on the orders of the Belarusian Ministry of Culture (Czosseck, Geers, 2009). All other known cases of internet censorship have involved the use of cyber tools such as DDoS attacks against Belarusian independent online media sites and websites related to reporting current affairs in Belarus.

Belarusian intelligence, although it has its own capabilities, works closely with Russian intelligence agencies. This cooperation includes cyber-espionage, cyber-attacks and information warfare campaigns aimed at opposing nations, dissidents or their political and strategic objectives. The involvement of Belarusian groups, possibly in support of or under the direction of Russian intelligence, highlights the depth of the relationship between the two countries' secret services.

The cooperation between Russian and Belarusian intelligence services in cyber operations highlights the deep-rooted alliance between the two countries, extending their cooperation into the digital sphere. Russian agencies such as the FSB and the GRU have been actively involved in cyber activities targeting Western targets, including espionage, disruption and disinformation campaigns. Belarus under President Lukashenko cooperates closely with Russia, including in security and intelligence efforts. The Belarusian KGB, although less visible in reports of international cyber operations, operates in tandem with Russian intelligence, indicating a united front in cyber efforts. This partnership has raised concerns among cybersecurity experts, government officials and international observers about the implications for global digital security and political stability. (The 5×5, 2022) Russian and Belarusian intelligence cooperation in cyber operations, particularly targeting Ukraine, has been highlighted in various analyses and reports. A prominent example of such cooperation is the hacker group with links to

Belarusian intelligence that is suspected to have carried out a cyber-attack on Ukrainian government websites. The group, known as UNC1151, is believed to have worked with or at the request of Russia, corrupting websites with threatening messages and installing destructive malware. This attack, which took place around 14 January 2022, was a cover for more serious actions behind the scenes aimed at disruption and intelligence gathering. (Polityuk P., 2022)

There are two main factors that could influence closer cooperation between the two countries in cyber operations: Russia's clear support for the Lukashenko regime since the 2020 Belarusian elections, and Russia's increasing lending to Belarus in recent years. These factors are probably why we are seeing Belarus give up its once closed territorial sovereignty to welcome the Russian forces invading Ukraine. Since Lukashenko has lost his legitimacy as President of Belarus and has been ostracised from closer ties with Europe, he is attracted to much closer relations with Russia. (The 5×5, 2022)

The Belarusian government has been linked to cyber-attacks against other countries. These specific incidents reflect the growing threat of cyber warfare by Belarus in the region.

- In 2020, foreign embassies in Belarus were attacked by a cyber-espionage group using internet service providers in Belarus. The perpetrator of the attacks is identified as "Moustached Bouncer", known since 2014 and believed to be acting on behalf of the Belarusian government (Kovacs, 2023).
- 2021 Cyber attack on Ukrainian government websites. A criminal group linked to Belarusian intelligence, known as UNC1151, is believed to have carried out a cyber-attack against Ukrainian government websites. The attack filled the websites with threatening messages. The group is believed to have been linked to Belarusian intelligence and has also been involved in cyber-espionage activities in Lithuania, Latvia, Poland and Ukraine, spreading narratives against the NATO alliance (Polityuk, 2022).
- In 2021, cyber-attack targeting Ukrainian military personnel. Belarusian hackers, identified as UNC1151, targeted the private email addresses of Ukrainian military personnel and associated individuals. They used password-stealing emails to hack into the email accounts of Ukrainian military personnel and then used compromised address books to send other malicious messages. The group was linked to the Belarusian military and was known for stealing and leaking sensitive information to influence public opinion, including targeting the NATO alliance (Satter, 2022).
- Another high-profile attack by the cybercrime group UNC1151 targeted numerous government and private sector entities, mainly in Ukraine, Lithuania, Latvia, Poland and Germany. Belarusian dissidents, media entities and journalists have also been targeted. The activities of this group are mainly in the interests of Belarus. The UNC1151 group's cyber-attacks were aimed at obtaining confidential information, and interestingly, no motive for financial gain was revealed (Roncone & all, 2021).

By carrying out cyber-attacks against its own citizens and other countries, Belarus has also become a target of cyber-attacks.

- In 2020, one fifth (19.02%, 2 million attacks) of all cyber-attacks in Europe targeted Belarus. The number of attacks increased especially during the 2020 presidential elections (Đorđević, 2020).
- DDoS attacks against Belarusian government websites in 2020 had increased. The attacks were seen as a digital protest against government actions and policies, leading to temporary disruption of online services. The attacks were aimed at depleting server resources. Some of these attacks were extremely effective, exceeding 200 Gbps in aggregate data, but were mitigated by the capabilities of the Belarusian internet service providers. The website of the Central Election Commission of Belarus was also one of the main targets of these attacks (E-Belarus.ORG).
- In 2022, the most significant attack targeted the Belarusian railway system, with the aim of disrupting the movement of Russian military equipment through Belarus. This attack was part of wider geopolitical tensions in the region and was characterised by its direct impact on physical infrastructure. The attack was undertaken by anti-government cyber groups within Belarus (Mohee, 2022), (Nair, 2022).

The IT sector in Belarus is recognised for its high competence and rapid growth. In 2019 About 54,000 people worked in Belarus (Husar, 2022). IT specialists, and by 2020 this has increased to around about 115,000 IT workers. The Belarusian IT sector exists separately from the internal Belarus industrial sector, focusing mainly on the export of IT services (Tolkachev & All, 2020). Belarus is renowned for having the best software engineers and programmers in the world due to its excellent education systems and strong science background (Starovoytova, 2020). The Belarusian IT industry was the fastest growing sector in the Belarussian economy, which became the

main engine of economic growth. Established in 2005, the High-Tech Park (HTP) has developed into the Silicon Valley of Belarus, demonstrating the country's potential in the technology industry (Irascu, 2023).

In recent years, a relatively large outflow of Belarusian IT specialists to western countries has been observed, but a considerable number of specialists still remain in Belarus. We cannot underestimate the potential of this country's IT professionals in supporting the cyber activities of the Belarusian government.

3. Cybersecurity Legal Background and Compliance Situation in Belarus

In this section of the paper, we will start to explain the legal aspects of cyber security and Belarus.

3.1 Legal Framework in Belarus

Cybersecurity as defined by ENISA in 2017 covers all aspects of the prevention, forecasting, tolerance, detection, mitigation, removal, analysis, and investigation of cyber incidents (ENISA, 2021). In the Republic of Belarus, there is no formal national cybersecurity strategy, there are no formal definitions of "cybersecurity" in the legislation, but many detailed provisions characterizing it are contained in various other regulatory documents (United Nations Institute). In the Republic of Belarus, there is more well-established term "information security", the National Security Concept of Belarus, approved by Decree No. 575 of the President of Belarus on 09.11.2010, defined "information security" as a condition to protect the balanced interests of the individual, society and the State from external and internal threats related to information and identifies information security as an independent component of national security (Cybercrime and cybersecurity strategies, 2018). The National Security Concept of Belarus formulates these national interests and includes the following aspects: shaping and gradually developing the Belarussian information society; having the Republic of Belarus as an equal participant in the world information relations; ensuring reliability and resilience of critical informatisation objects (this can be related to the Western concept of Critical Infrastructure).

In August 2017 Resolution No. 607 was approved "Concept of Union State Program on Information Security", which entered into force in 2018. The Concept included the introduction of the definitions of "information sovereignty" and "information neutrality". The Concept of Union State Program refers to the information sovereignty as "the indispensable and exclusive right of the state to independently shape the rules of ownership, use and administration of national information resources; to conduct independent foreign and domestic information policy; to shape the national information infrastructure; to ensure information security (International Information Security). Therefore, information sovereignty of Belarus has been made into a national priority. One of the main goals declared by the Concept of Union State Program is to ensure the rule of the Belarus state over its information domain. This immediately sidelines other areas of consideration, such as the rights of the citizens and international commitments. The technical section of the 2017 Concept of Union State Program includes measures ensuring security of the information infrastructure and of the national segment of the Internet; countering cybercrimes; ensuring security of public information resources, including of state and public secrets; and protecting personal data from unauthorized access.

In March 2019, the Doctrine of Information Security of the Republic of Belarus was approved, which proclaimed information sovereignty, respect for the digital sovereignty of other countries and the pursuit of a peaceful foreign information policy (International Information Security).

In February 2023 the Supreme State Council of the Union State approved the Concept of Information Security of the Union State (Ministry of Foreign Affairs BY). The concept document was developed in close collaboration of the offices of the Security Councils, Foreign Ministries and other authorities of the two countries – Belarus and Russia. The concept document seeks to create a solid legal foundation to respond to modern information challenges and threats.

Some other regulatory frameworks in Belarus covering data protection and cybersecurity obligations includes the Strategy of development of informatisation in Republic of Belarus for 2016-2022 adopted in 3 November 2015 (No.26), National program of development of digital economy and information society for 2016-2020 adopted in 23 March 2016 (No. 235) and other Laws and the Edicts of the President related to data/information protection. Cybersecurity in Belarus is also covered by a range of specific legal acts relating to the particular categories of information systems and its owners. For example, the Banking Code of the Republic of Belarus dated 25.10.2000, Rules on Rendering Services Connected to Creation and Placement of Digital Signs (Tokens) and Related Transactions approved by the Supervisory Board of the High Technologies Park. Specific legislation on cybercrime has been enacted through the Criminal Code. Chapter 31 of the Criminal Code deals with

cybercrime offences such as the unauthorised access to computer information; deletion, blockage or modification of computer information; non compliance with the rules regulating exploitation of computer system or networks (Уголовный кодекс Республики Беларусь). While substantive cybercrime offences are mostly in place, there are significant gaps in terms of implementing procedural powers under the Budapest Convention on Cybercrime (Cybercrime and cybersecurity strategies, 2018).

3.2 International Cooperation

Belarus has not yet acceded to the Budapest Convention on Cybercrime (ETS 185) but has expressed a strong interest in accession. The Council of Europe, under the Cybercrime@EAP II joint project with the European Union, supported a workshop aimed at promoting "the harmonisation of Belarusian legislation with the Budapest Convention on Cybercrime" (Harmonising legislation with the Budapest Convention, 2018). In 2020 Belarus was ranked in 89th place the ITU global cybersecurity index (Global Cybersecurity Index, 2020).

Current practices of international cooperation with Belarus are mostly involving supporting mutual legal assistance requests. The timeframes for processing and execution of incoming mutual legal assistance requests are rather long and delays are experienced mostly due to large requests requiring translation (considered to be particularly problematic) and/or need to clarify ambiguities in cases of incomplete/low-quality requests; triage of mutual legal assistance requests not performed or based upon informal criteria and is not uniform in application (Cybercrime and cybersecurity strategies, 2018). In addition, the lack of sufficiently clear and proper basis in national law to cooperate directly with multinational service providers (MSPs) in criminal cases, being one of the major reasons for declining cooperation (Cybercrime and cybersecurity strategies, 2018). There are also obvious examples in other than computer related/cybersecurity criminal cases that Belarus is not a cooperating country (alfa.lt, 2013). On the other hand, since February 2023 when the concept document was developed in close collaboration between Belarus and Russia, two countries began to cooperate in order to protect the national interests of the Union State[2] members in the media landscape. Russia and Belarus developed joint guidelines for a coherent state policy and for public relations in the field of information security. Both countries also set the framework for improving the information security systems of the two states.*3.3. Institutional framework*

The main regulatory authorities relating to the generally applicable cybersecurity-related laws are: Operations and Analytics Center under the President of the Republic of Belarus and Ministry of Communications and Informatization of the Republic of Belarus. These institutions are mainly responsible for the implementation of a unified state policy in the sphere of data protection, promotion of creation of information technologies, information systems and information networks; technical regulation and standardization of information resources, information systems and information networks; coordination of activities of state bodies in the cybersecurity sphere; coordination of formation and state registration of information resources and similar.

4. Belarus Cyber Case Studies: Pro-Government and Anti-Government Hacking Groups

This section of the paper will focus on different hacking groups that exist in Belarus.

4.1 Belarus Cyber Partisans

The "Belarus Cyber Partisans" (also known as "BCP") is a hacktivist group that has gained attention for its activities related to the political situation in Belarus. The Belarus Cyber Partisans are a hacktivist group that emerged in opposition to the regime of Belarusian President Alexander Lukashenko. They gained prominence by launching cyber-attacks on Belarusian state critical infrastructure, leaking sensitive information, and disrupting government websites. The group claims to be fighting for freedom and democracy in Belarus, where widespread protests against alleged electoral fraud erupted in 2020. Their activities have raised concerns about the vulnerability of critical infrastructure to cyber-attacks. The Belarusian government has condemned their actions, accusing them of terrorism and foreign backing.

[2] The union of Russia and Belarus. Signed by the heads of states in 1999. The Agreement on Establishment of the Union State of Belarus and Russia sets up a legal basis for integration between the two countries.

The Belarus Cyber Partisans claimed several significant cyber activities. While the fame or significance of these actions can be subjective and might change over time, here are four notable activities attributed to the group:

1. Critical Infrastructure Attacks: They claimed responsibility for several attacks on Belarus's railway system. One such attack temporarily disrupted ticket sales (Bajak, 2022), while another aimed at halting train movement, though it was unclear how successful that was (theguardian.com, 2022), (railway-technology.com, 2022).
2. Data Leaks: The group reportedly leaked data from the Belarusian police and interior ministry databases. This exposed personal information of police officers, which the group claimed was to hold the police accountable for alleged acts of violence against protestors (zdnet.com, 2020). Another examples: a series of hacks on Belarus's government by pro-democracy activists has uncovered details of apparent abuses by security forces, exposed police informants and collected personal data on top officials including a son of President Alexander Lukashenko (washingtonpost.com, 2021), (currenttime.tv); the activists also hacked into the database of all criminal and administrative cases in Belarus and downloaded their archives (euroradio.fm, 2023).
3. Website Defacements: The group took over various government websites, displaying protest messages and replacing official content with images and slogans supporting the opposition (Kazharski, 2021).
4. Interception of Official Communications: They claimed to have wiretapped audio of foreign embassies, consulates and other calls in Belarus gathered surreptitiously by the Belarusian Ministry of Internal Affairs (cyberscoop.com, 2023).

According to George 2023), the hacktivist organisation, Cyber Partisans, partnered with the Kastuś Kalinoŭski Regiment, an anti-Russian Belarussian military group made up of volunteers fighting for Ukraine. As Belarus has been used by Russia to bolster its invasion operations, the partnership between Belarussian partisan groups is a strategic relationship that reinforces cyber defense and offense efforts. The partnership related to coordinated actions aligning virtual attacks with physical attacks, with the aim of producing more effective results (George, 2023). Thus, the Belarusian partisans are also acting in a hybrid way to extend their real influence. A number of cases of Belarusian cyber-partisans collaborating with journalists have also been documented. Hackers with access to sensitive information has been sharing it with journalists. Although the ethicality of such activities has been questioned in press (thefix.media, 2022), it should be mentioned that Belarusian cyber-partisans have significantly increase the publicity of their activities and the data they collect have been reported by the media around the world.

4.2 Pro-Belarus Hackers

Hackers supporting the Belarusian regime usually acting to counteract opposition movements and reinforce President Lukashenko's grip on power, especially after the contentious 2020 election. These cyber actors have targeted opposition websites, activists, and disseminated pro-government propaganda online, etc. They also target countries that oppose Russian/Belarusian actions and policies. Most often hackers are reluctant to make information about their activities public, so there is much less public information. Nevertheless, we can categorise their activities as follows:

1. Disinformation Campaigns: These are efforts to spread false or misleading information online. Given the political unrest and tensions in Belarus, especially after the 2020 presidential elections, pro-Belarus entities might use disinformation to control narratives, discredit opposition, or influence international perceptions. Such attacks can be directed both within a country and against other countries. As part of the campaign in 2023, the hackers, who cybersecurity experts also refer to as UNC1151, sent fake messages to Polish citizens about potential recruitment to the Lithuanian-Polish-Ukrainian brigade, a multinational military focused on conducting peacekeeping and humanitarian operations. The hackers also made false claims that the brigade will take part in military operations in Ukraine. The campaign is just the latest in a series of disinformation operations conducted by Russia and Belarus aligned hackers. The Polish state authorities claimed their goal is to destabilise the situation in the country (therecord.media, 2023).
2. Web site defacements: this involves unauthorised modifications of web pages, typically replacing the original content with the hacker's message or propaganda. Given the political context, opposition or journalist websites could be potential targets. We have also seen these groups target governments outside Belarus. For example, Ukraine accused a Belarusian-linked hacker group in 2022 of attacking its government websites using Russian intelligence linked malware (tickernews.co, 2022).

3. Data breaches: This relates to the unauthorised access to sensitive data, potentially followed by public release of that data. This can be used as a tactic to intimidate, embarrass, or discredit targets, especially opposition figures or entities perceived as threats. Hackers from Belarus were targeting the private email addresses of Ukrainian military personnel “and related individuals” to gain access of Ukrainian soldiers’ email accounts and using their compromised address books to send further malicious messages (euronews.com, 2022).

As far as the recent activities of pro-Belarusian government hackers are concerned, it should be noted that their main "focus" is on Ukraine[3]. Thus, as a separate group, the authors would like to highlight pro-Belarusian hacker attacks against Ukraine (especially after the Russian invasion of Ukraine beginning in 2022). Hackers linked to the Belarusian government, known as GhostWriter, targeted government, military, and civilian entities in Ukraine and Poland from at least April 2022, according to a report by cybersecurity firm Cisco Talos. They have been using malicious Microsoft Office attachments, including disguised Excel and PowerPoint files, the attackers deployed malware to steal information and gain remote system access (therecord.media, 2023). The various methods are that are used intend to undermine Ukraine and other countries that support them. This is evidenced by publicly available cases (reuters.com, 2022).

While conducting research, the authors sought to find out the connections between Belarus pro-government hackers and Russian APT groups[4]. Several such groups operate in Russia, for example, Berserk Bear, Fancy Bear, Gamaredon and others. Belarusian pro-government hackers and their links with Russian APT groups could highlight a concerning trend in the cyber domain, particularly in the context of international geopolitics and cybersecurity. The direct links between Belarus pro-government hackers and Russian APT groups were not explicitly detailed in the public sources. For example, one of the cyber analysts in 2022 was quoted as follows: "Though we cannot rule out Russian contributions to either UNC1151 or Ghostwriter[5] activities, we have not yet identified evidence of any collaboration between Russian APTs and UNC1151” (Belarus threat.., 2022). But the broader context of cyber threats and state-backed cyber activities, including those attributed to Russia, provides a relevant backdrop. The escalation of cyber threats, such as ransomware attacks and exploitation of vulnerabilities, underscores the complexity of the cyber threat landscape where state-backed or state-affiliated actors could potentially collaborate or share tactics. The landscape of cyber warfare and cyber espionage is continually evolving, with state actors and their affiliates playing significant roles in targeting adversaries or supporting geopolitical aims. Therefore, it cannot be claimed that there are no connections between Belarus pro-government hackers and Russian APT groups, and the relevant connections are the object of further research.

4.3 Comparison: Belarussian Cyber-Partisans and Pro-Belarussian Hacker.

The authors compare the activities of the different Belarusian cyber-partisans with the pro-Belarusian hackers:

Table 1:

	Belarussian Cyber-Partisans	Pro-Belarusian hackers
Motivation	The Belarus Cyber Partisans engage in hacktivism to challenge the Lukashenko regime, advocating for democratic reforms and transparency in response to alleged electoral fraud and state-sanctioned violence.	Pro-Belarus hackers are driven by a desire to defend the Belarusian government and its national interests, countering perceived external threats and internal dissent.
Targets	They have primarily targeted Belarusian state infrastructure, like railways, and have leaked data from government databases, such as the police and interior ministries.	Their likely targets include opposition political websites, independent media, and communication channels used by activists or dissidents. Foreign governments who

[3] And, in some cases, against other states that support Ukraine.

[4] **Russian advanced persistent threat groups.**

[5] Ghostwriter, also known as UNC1151, is a hacker group allegedly originating from Belarus.

	Belarussian Cyber-Partisans	Pro-Belarusian hackers
		support the opposition in Belarus and the Ukrainian government.
Operating area	They operate both inside and outside if Belarus.	Mostly external to Belarus: pro-Belarus attacks are usually directed at Ukraine (especially after the war started), but also aimed at NATO countries, mainly the Baltic States.
Tactics, techniques, *modus operandi*	Their tactics have been centered on data breaches, infrastructure attacks, and public disclosures. They have targeted state systems, leading to service disruptions and information leaks.	Historically, pro-government hackers have employed disinformation campaigns, DDoS attacks, and espionage-based cyberattacks. Their focus would typically be on silencing opposition voices and protecting state interests.
Origins and backing	They emerged from grassroots hacktivist movements, potentially collaborating with other global hacktivist entities.	Likely to be state-sponsored or backed by entities with close ties to the Lukashenko regime.
Cooperation	They usually act alone. However, journalists are involved in publicising activities and results. Cases of hybrid cooperation with local anti-Belarus military groups have also been observed.	Pro-Belarus cyber-operations are involved cooperation with Russian and Chinese hackers. Often, pro-Belarus groups are involved in disinformation campaigns.

5. Conclusions

1. Belarus has experienced significant challenges related to cybercrimes and online censorship, particularly under President Alexander Lukashenko's regime. The government has utilised internet censorship and undertook DDoS attacks as tools against political dissent and opposition, often without legal justification and in violation of Belarusian constitutional laws. This repression escalated notably following the disputed 2020 presidential elections. Furthermore, Belarus has been implicated in cyber-attacks against other countries, with groups like UNC1151 conducting espionage and disruptive activities across Europe. Conversely, Belarus itself has been a significant target of cyber-attacks, especially during politically sensitive periods.
2. Belarus has developed a legal framework in terms of focusing on information security asset (in the western context described as critical infrastructure). The Belarus government has also developed legal frameworks to allow the government to censor online content with Belarus. A new challenge is the geopolitical union with Russia, which also influence the creation of new future legal frameworks.
3. Belarus' close relationship with Russia extends into the realm of cyber and hybrid threats, where Belarusian actors have been implicated in cyber-attacks that align with Russian geopolitical interests, especially against neighbouring countries and NATO members. This collaboration often involves coordinated cyber espionage, disinformation campaigns, and attacks on critical infrastructure, reflecting a shared strategy to exert influence and disrupt perceived adversaries. Additionally, Belarus' cyber capabilities and infrastructure may be leveraged by Russian entities to launch cyber-attacks, making it a significant player in the broader landscape of regional cyber threats.

References

'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup, 2022 // https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

«Уголовный кодекс Республики Беларусь» – тематические подборки НПА на Pravo.by. (n.d.). https://pravo.by/document/?guid=3871&p0=hk9900275

Belarus hackers attack train systems to disrupt Russian troops, 2022 // https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/

Bajak, F. Belarus hacktivists target railway in anti-Russia effort, January 25, 2022 // https://apnews.com/article/russia-ukraine-technology-business-moscow-belarus-fe6dd5e3ff9ec0718b6448e770c15c29

Belarus-linked hacking group targets Poland with new disinformation campaign, April 19, 2023 // https://therecord.media/ghostwriter-belarus-hacking-group-targets-poland-disinformation

Belarus-linked hacks on Ukraine, Poland began at least a year ago, report says, July 13, 2023 // https://therecord.media/poland-ukraine-ghostwriter-attacks-belarus

Belarus threat group in Ukraine 'bomb alert' cyberattack, July 21, 2022 // https://cybernews.com/cyber-war/belarus-threat-group-in-ukraine-bomb-alert-attack/

Belarus: Harmonising legislation with the Budapest Convention. (2018, April 26). Cybercrime. https://www.coe.int/en/web/cybercrime/-/harmonising-legislation-with-the-budapest-conventi-1

Belarusian cyber partisans hack into important state database, March 8, 2023 // https://euroradio.fm/en/belarusian-cyber-partisans-hack-important-state-database

Belarusian hacktivist group releases purported Belarusian wiretapped audio of Russian embassy. June 14, 2022 // https://cyberscoop.com/belarusian-hacktivist-group-releases-purported-belarusian-wiretapped-audio-of-russian-embassy/

Belarusian journalists collaborate with the hacktivists who have a lot of sensitive information — how does it work and is this ethical? October 25, 2022 // https://thefix.media/2022/10/25/belarusian-journalists-collaborate-with-the-hacktivists-who-have-a-lot-of-sensitive-information-how-does-it-work-and-is-this-ethical

Criminal code of Belarus, 1999 https://pravo.by/document/?guid=3871&p0=hk9900275, art. 349-355

Cybercrime and cybersecurity strategies in the Eastern Partnership region. 2018. CyberCrime@IPA (coe.int), page 28.

Czosseck, C., & Geers, K. (2009). Belarus in the Context of European Cyber Security. The Virtual Battlefield: Perspectives on Cyber Warfare, 3, 156.

Disinformation campaigns, cyber attacks, economic pressures, military posturing, political interference, etc.

Đorđević, N. (2020, September 10). Cyberattacks in Belarus compound discontent in country's IT sector - Emerging Europe. Emerging Europe. https://emerging-europe.com/news/cyberattacks-in-belarus-compound-discontent-in-countrys-it-sector/

E-Belarus.ORG | Internet Shutdown in Belarus / Official version: DDoS Attacks. (n.d.). https://e-belarus.org/news/202008121.html#:~:text=A%20particularly%20large%20number%20of,and%2023%3A20%20on%209%20August

ENISA overview of cybersecurity and related terminology. Results of series of national workshops Eastern Partnership countries PGG 2018: Cybercrime@EaP project February - May 2018. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

G. Roncone, A. Wahlstrom, A. Revelli, D. Mainor, S. Riddell, B. Read. UNC1151 Assessed to have Links to Belarusian Government. Mandiant. https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government

George J. J. Considering Cyberwar Efficacy: Is Mitigation Possible? Georgetown Journal of International Affairs. September 11, 2023 // https://gjia.georgetown.edu/2023/09/11/considering-cyberwar-efficacy-is-mitigation-possible/

Hackers leak details of 1,000 high-ranking Belarus police officers, 2020 // https://www.zdnet.com/article/hackers-leak-details-of-1000-high-ranking-belarus-police-officers/

How Belarus's 'Cyber Partisans' exposed secrets of Lukashenko's crackdowns // https://www.washingtonpost.com/world/europe/belarus-hack-cyber-partisans-lukashenko/2021/09/14/5ad56006-fabd-11eb-911c-524bc8b68f17_story.html

Global Cybersecurity Index 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Information Security - Ministry of Foreign Affairs of the Republic of Belarus. (n.d.). https://mfa.gov.by/en/mulateral/global_issues/inform/

International Information Security - Ministry of Foreign Affairs of the Republic of Belarus. (n.d.). https://mfa.gov.by/en/mulateral/global_issues/inform/

Kazharski A. Belarus' new political nation? 2020 anti-authoritarian protests as identity building. New Perspectives 2021, Vol. 29(1). P. 76 // https://journals.sagepub.com/doi/10.1177/2336825X20984340

Kovacs, E. (2023, August 11). Moustached Bouncer: Foreign Embassies in Belarus Likely Targeted via ISPs. SecurityWeek. https://www.securityweek.com/moustachedbouncer-foreign-embassies-in-belarus-likely-targeted-via-isps/

Ministry of Foreign Affairs of the Republic of Belarus, https://www.mfa.gov.by/en/press/news_mfa/cac0ee302b706cd8.html

Mohee, A. (2022). Cyber war: The hidden side of the Russian-Ukrainian crisis.

Nair, S. (2022, March 23). Belarus hackers attack train systems to disrupt Russian troops. Railway Technology. https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/

O'Neill, P. H. (2021, October 26). Hackers are trying to topple Belarus's dictator, with help from the inside. MIT Technology Review. https://www.technologyreview.com/2021/08/26/1033205/belarus-cyber-partisans-lukashenko-hack-opposition/

Outsourcing in Belarus - Information & Technology Statistics. (n.d.). https://techbehemoths.com/blog/it-outsourcing-belarus

Pavlyuchenko, F. (2009). Belarus in the context of European cyber security. In The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 156-162). IOS Press.

Polityuk, P. (2022, January 16). EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack. Reuters. https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

Prokuroras, vadovaujantis Sausio 13–osios žudynių bylai: Rusija ir Baltarusija nebendradarbiauja. https://www.alfa.lt/straipsnis/15074922/alfalt/

Rusinaite V. Russia's policy towards Belarus: Controlling more, giving back less. December 2021. [20211220-Hybrid-CoE-Strategic-Analysis-30-Russias-policy-Belarus-WEB.pdf (hybridcoe.fi)]; p. 4

Satter, R. (2022, February 25). Ukraine says its military is being targeted by Belarusian hackers. Reuters. https://www.reuters.com/world/europe/ukraine-says-its-military-is-being-targeted-by-belarusian-hackers-2022-02-25/

Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data // https://en.currenttime.tv/a/seeking-change-anti-lukashenka-hackers-seize-senior-belarusian-officials-personal-data-/31392092.html

The Belarus IT Industry: One of the Best Talent Hubs in the World | Satellite Innovations. (n.d.). https://www.satelliteinnovations.io/blog/the-belarus-it-industry-one-of-the-best-talent-hubs-in-the-world#:~:text=The%20average%20developer%20in%20Belarus,educational%20systems%20and%20technical%20roots

The IT Industry in Belarus: General Portrait. (n.d.). https://techbehemoths.com/blog/the-it-industry-in-belarus-2021-general-portrait

Tolkachev, S., Быков, Morkovkin, D., Borisov, O. I., & Gavrilin, A. V. (2020, January 1). Digitalization of manufacturing in Russia, Belarus and the European Union. IOP Conference Series. https://doi.org/10.1088/1755-1315/421/3/032041

Ukraine says its military is being targeted by Belarusian hackers, February 25, 2022 // https://www.euronews.com/next/2022/02/25/us-ukraine-crisis-cyber

Ukraine suspects group linked to Belarus intelligence over cyberattack, January 16, 2022 // https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

United Nations Institute for disarmament research. Cyber Policy Portal. (n.d.). https://cyberpolicyportal.org/

S. (2022, July 7). The 5×5—Russia’s cyber statecraft. Atlantic Council. https://www.atlanticcouncil.org/commentary/the-5x5-russias-cyber-statecraft/

Polityuk P. EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack (January 16, 2022), https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/