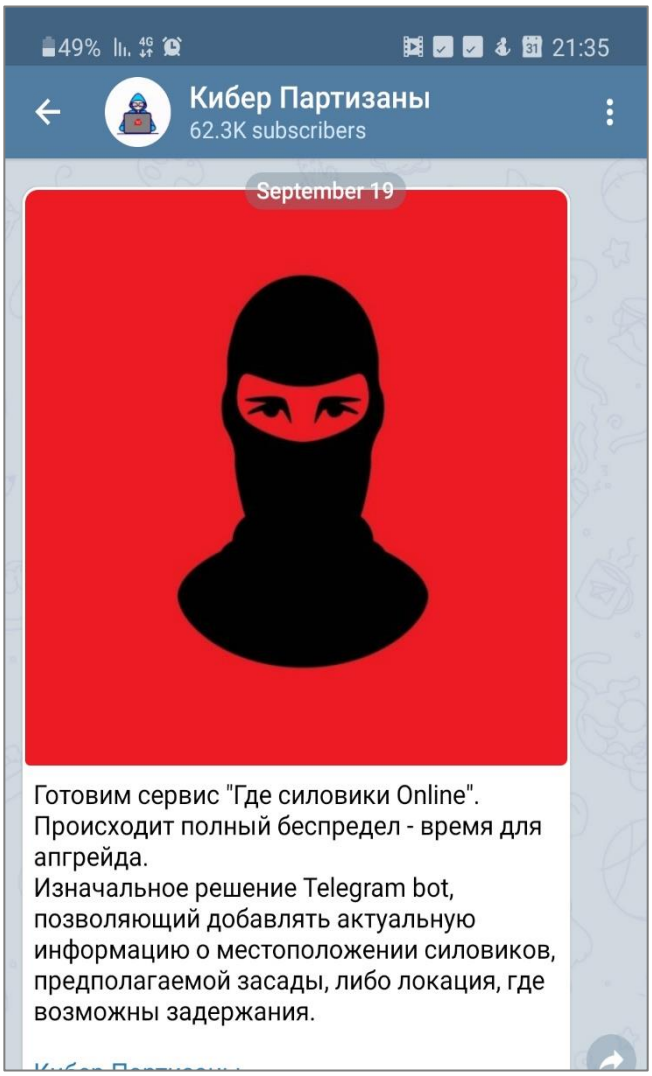
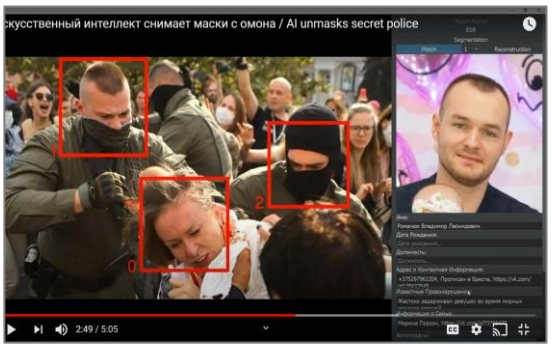
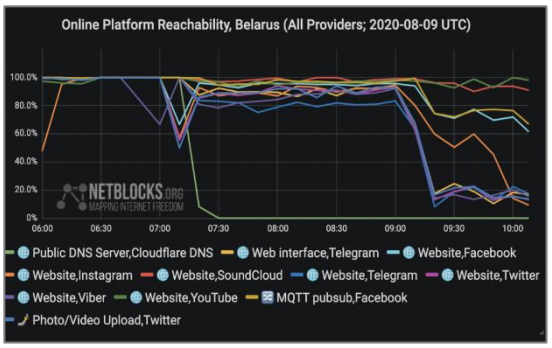






“Cyber Partisans” – The Belarus Elections, 2020

Use of the benefits of Information Technology and Cyber – Case Study Presentation

Evyatar Grinshpun, October 2020

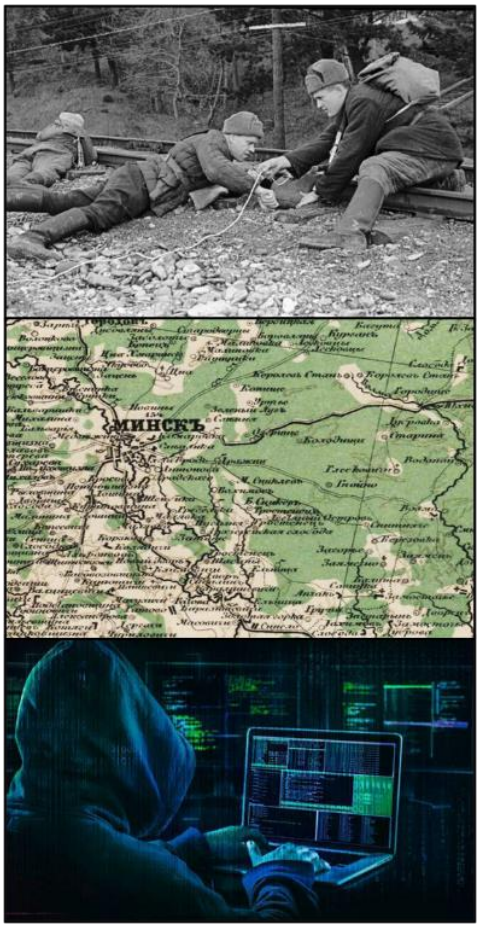
Introduction

As part of the global technological development, information and communication technology is used more and more. Such technologies interact with current processes, modify them and even create new ones.

Frequently, when we are in the middle of change – we are unable to observe it happening. Sometimes a certain perspective is required in order to realize it is happening now or had already happened.

Throughout human history, information has been a valuable, sometimes even a decisive factor in various types of confrontations: military, economic or political. In 2020, Belarus had General Elections. These elections were very stormy, with the incumbent president, Alexander Lukashenko (Аляксáндр Лукашэ́нка), who's already ruled Belarus for 26 years, fighting several new candidates whose aim was to overthrow him and lead far reaching reforms in that state. Even though the formal elections ended on 8 August 2020, they ignited a tumultuous, wide-ranging wave of protest that hasn't abated to this day.

During that time in Belarus, the use of information technology and cyber warfare has grown constantly, with various opposition forces using them to gain an advantage against government forces, local and international public opinion. One of the conspicuous technological moves was the setting up of "Cyber Partisans" units ("Кибер Партизаны"). This technology-based protest aims, in a similar way to the old partisans, to damage and disrupt the existing regime. The term *partisans* is well known in Belarus,



From Partisans to "Cyber Partisans"

suggesting the Second World War partisan units who conducted a popular, and mostly righteous, struggle against the occupiers.

Even if some of their methods have already been seen before, we can see that using technology for this struggle covers a wide scope and is quite unique.

The story of the "Belarus 2020 Elections" tells us how technology is implemented in society and used for a wide variety of purposes.

First, in order to understand the unique technological characteristics of this story, here is a relatively wide-covering introduction to the internal and geopolitical situation of Belarus.

A few comments before we start

As with any geopolitical event, this is a complex story with many conflicting interests: Those involved are government agencies, opposition forces, various elements inside the country, adjoining countries such as Russia and Poland, NATO countries such as France and Germany, Western countries further away such as the USA, and others. This article is based on media stories, official state websites, social media and the foreign press. We placed a special emphasis on **domestic media** run by opposition forces using social media, mainly various Telegram channels.

At a time of a wide-ranging use of media manipulation and fake news, it can be assumed that such tactics have also been used by those involved in this story. It is important to note that the **events described below are still ongoing**, and we lack any time perspective yet.

At the same time, it makes sense to highlight the events even at this stage, offering readers the option to analyze them while trying to follow the processes that are still ongoing.

Introduction

Belarus (Рэспубліка Беларусь) is an independent country in Eastern Europe. It borders Russia, Ukraine, Poland, Lithuania and Latvia. Until 1991 it was part of the Soviet Union. During the period leading to its independence, Belarus had absorbed the Russian culture, mentality, language and various modes of conduct. Even today, it maintains a deep and meaningful economic, cultural and military relationship with Russia.

Its population is 10 million, of whom 80% are Belarussian and 15% are Russian. The most common language is Russian, with Belarussian being the official language. It has a typical Eastern European climate and is relatively well-developed industrially. Geopolitically, the Belarussian foreign policy is close to that of Russia, which believes that Western countries are destabilizing regional and global stability. In recent years, a long debate has been going on about a possible union between the two countries.

Belarus defines itself as a republic, with a president who has very wide-ranging powers. He acts as Commander in Chief of the country's armed forces and appoints the President of the Constitutional Court as well as half of its judges. The President appoints his Prime Minister, who then appoints government ministers. The Belarussian parliament is weak and does not have real impact on the state. Elections take place every 5 years. Since 1994 (for 26 years!), Belarus President has been Alexander Lukashenko, who was elected repeatedly with a large majority. His rule seems to be very centralist in nature. For years, opposition leaders and various European countries have claimed that the Belarus elections are undemocratic and pre-decided. The elections results of

the past ten years have not been recognized by the European Union and the USA.

Throughout Lukashenko's rule, he has strongly invested in strengthening OMON, the country's Special Purpose Police Detachment (Атрад міліцыі асобага прызначэння). It was claimed on many occasions that these forces spearhead his regime's continued survival through the repression of the opposition and guaranteeing Lukashenko's continued re-election.

The August 2020 elections

Since 1994, Lukashenko won all elections. On 8 August 2020, immediately after the elections, the central election committee published the preliminary results: Lukashenko wone 84% of the votes, while the opposition's main candidate Svetlana Tsikhanouskaya won 10%.

After that announcement, a wave of protests erupted all over the country. The opposition declared that the elections has been falsified, and demanded the president to step down. Ever since that day, the opposition has attempted to disable the routine of the country while organizing mass protests that are still ongoing.

Elections 2020

On the other end, the incumbent President, supported by the police, the military and special forces, continues to dig in while aiming to violently repress the protests. This includes arrests, investigations, torture and the use of lethal ammunition.

There are some unique elements of the 2020 elections:

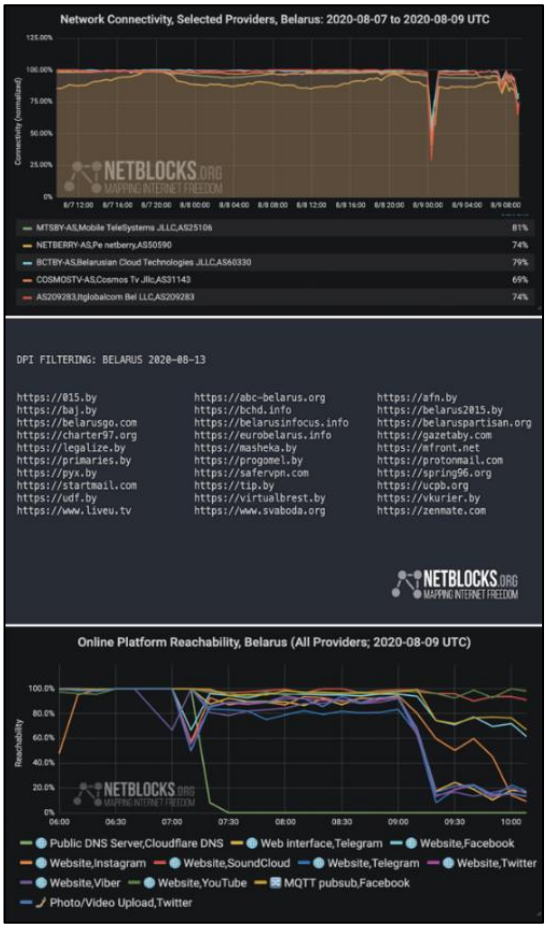
1. The President's sheer scorn of the medical implications of the Covid-19 epidemic and the economic decline that followed.
2. Consistent abuse of opposition leaders who wished to run against the President in the elections – through a denial of their right to run for office, long prison sentences and deportations.
3. Not authorizing the European Union to send observers to the elections.
4. Very extreme results of the election victory (80% vs. 10%).
5. Brutal violence since the protests had begun, with everything being documented, published and echoed in social media.

The regime restricts access to information

Just a week after the opposition's declaration that it does not accept the election results, the Belarus internet space suffered considerable disruptions.

This included blocked access to news sites, social media, E-mail and massaging services.

At the same time, government forces started a range of violent oppression moves against protesters, including the use of live ammunition, mass arrests, road blocking, and investigations and torture of those arrested.



NetBlocks publication

NetBlocks is organization which aims to monitor the global internet in order to detect government-oriented manipulations, managed to identify some interventions by the Belarus

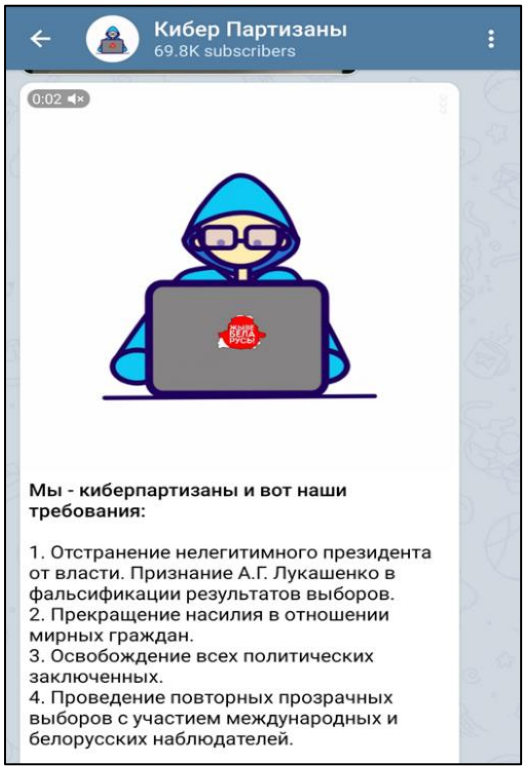
government: Changed routing, blocked access to social media and specific IPs and domains; and blocking specific search terms.

This blocking and restriction campaign of the internet had indeed succeeded, creating a media vacuum for about one week. These obstructions also prevented effective communication between opposition activists, and badly affected the organizing and coordinating of protests via social media. After about a week, once the disruptions had stopped, the country was shocked by the reports, images and videos showing the conduct of the Belarus security forces.

"Cyber Partisans"

One of the most conspicuous examples of the struggle against the regime is the creation of "Cyber Partisans". It all came together a month after the elections and has become a central focus of cyber activities against the country's central government. The group's name is not accidental. In Belarus, the term "partisan" connotes a heroic popular struggle during the dark period of the Second World War.

Most of the group communication is based on a specific channel in Telegram. Today it has over 70,000 subscribers.



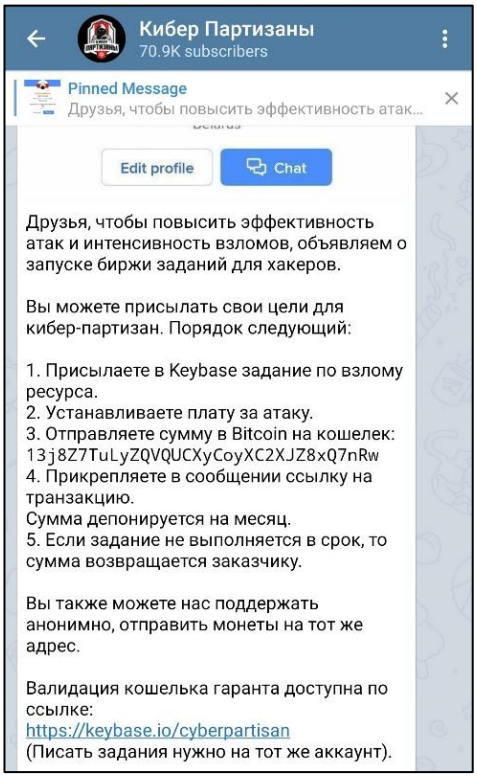
Official Telegram channel

Four demands were published by this group:

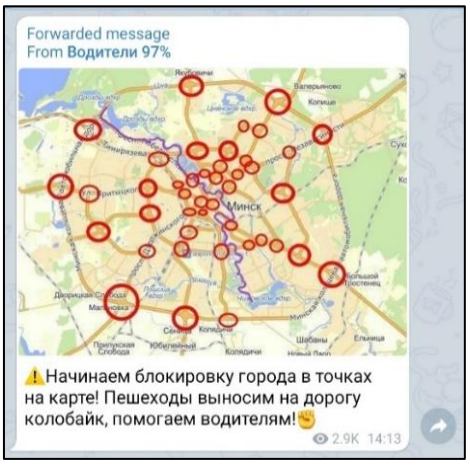
1. Dismissal of the President and a confession that the election results have been falsified.
2. Halting all violence against protesters.
3. Immediate release of all political prisoners.
4. Having re-elections with international observers.

The main actions performed by the "Partisans" include:

1. Economic damage to government institutions by disabling the national online payment services. This also damaged online payments of customs fees.
2. Visual damage to government websites. Among the more prominent events, the Ministry of the Interior website was hacked. Also, the capital's news website was hacked and a message implanted there about the President being wanted for murder.
3. The "Cyber Attacks Exchange" – in order to maximize the targeting, scope and effectiveness of the cyber attacks, the group initiated a kind of "Cyber Attacks Exchange". This works like this: anyone can suggest a target for attack, define the price they're willing to pay for achieving it, and place a Bitcoin deposit with the Exchange administrators. Should the target not be attacked within one month – the attack service customers gets their money back. If an attack took place – the money would go to the person who did it.
4. Much use of GIS infrastructures as a kind of Command & Control system to manage the locations of road blockages and demonstrations.
5. Much effort had been invested in exposing the details of members of the security forces and OMON (see definition above). The security forces



"Cyber Attacks Exchange"



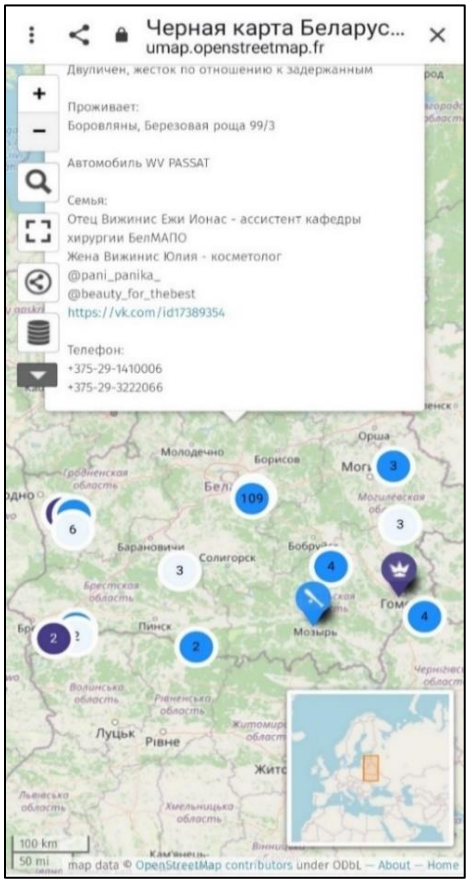
Map of roadblocks

involved in breaking down the protests wear balaclavas and display no means of identification.

The group hacked the state security forces' website and started publishing personal details of their personnel, including their families. This was aimed at placing public pressure on these people.

"Black Map of Belarus"

6. The group runs a project called "Black Map of Belarus". It is based on the Google Maps platform and constitutes an up-to-date geographical database of security forces personnel. It is open to public access and includes: full personal details, including their address and means of contact; which oppression activities they took part in and what was their role there; were they documented; and full details of their families.



"Black Book of Belarus"

7. A similar project along the same vein is "Black Book of Belarus". This project collects and maintains personal details, mainly photos, of security personnel, which were extracted from social media. The project aims at placing pressure on them and get the public to contact them directly through as many channels as possible.
8. "The Partisans" also hack the websites of the country's main TV channels to broadcast content the central government tries hard to censor, mainly

documentation of violence during demonstrations and the physical injuries of protesters.

9. "The Partisans" publicly call on IT network administrators working for the state to give them access the state's databases or leak such information themselves.
10. Another interesting area is the use of "The Wisdom of the Crowds" in order to map the deployment of street cameras in the capital. Activists are promoting the use of a public infrastructure on which anyone can accurately mark the location of street cameras, adding the address and the picture as well as the camera type and it's viewing angle. Such endeavor allows protesters to plan routes for their demonstrations, be careful in certain areas and even use those cameras for their own documentation and other needs.
11. On top of all this, "the Partisans" had created a "unique cyber community" which have shared cloud infrastructures, tools and code, technical tips, use of VPNs, open source systems for the creation of distribution platforms, channels and end-to-end encrypted email services. This community also shares amongst its members some lessons learnt, for example which IT

Publicly call on IT administrators

Public management of street cameras based on The Wisdom of the Crowds

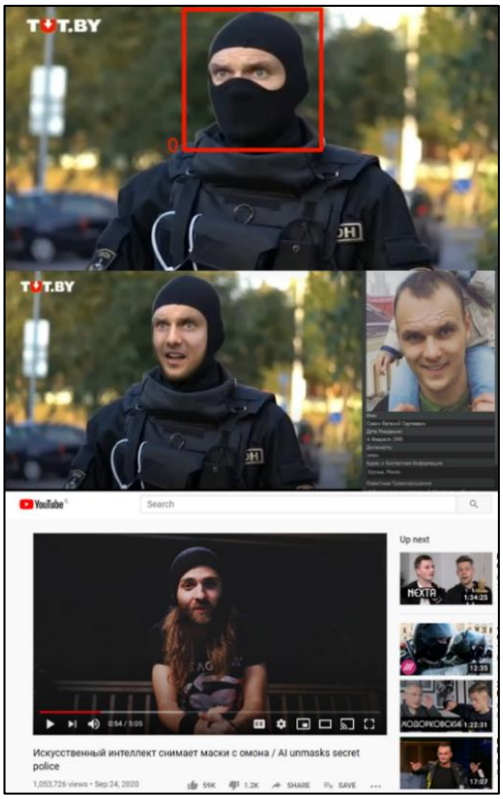
security platforms are used by the institutions who are under attack. In some cases, shared project development through GitHub code sharing has also been tried.

This is a lively and vibrant community, whose knowledge sharing practices definitely enhance its effectiveness.

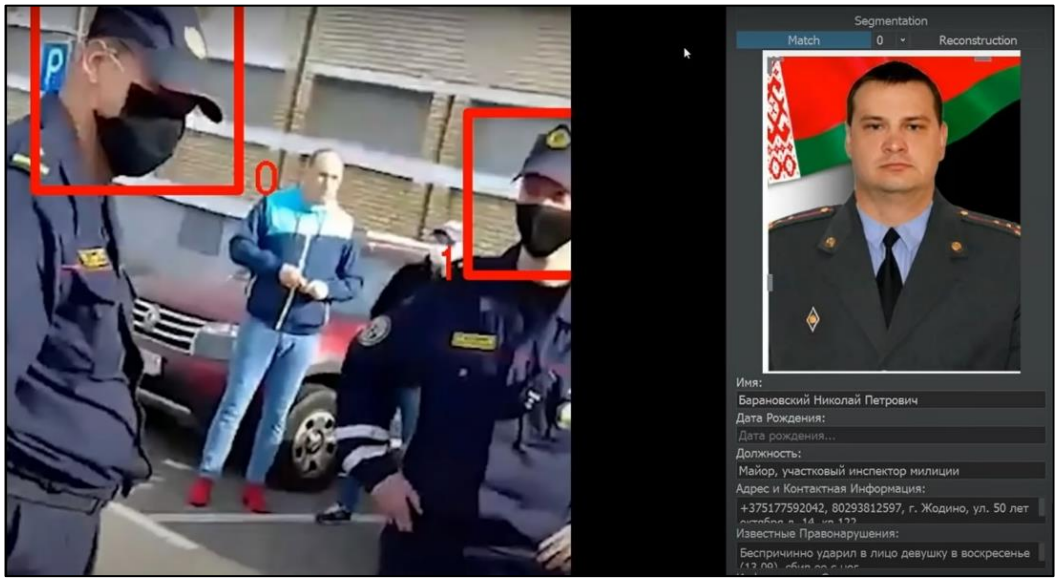
Activation of data extraction systems

One of the most conspicuous acts of the government forces is their efforts to hide their identities. The opposition activists announced that they'd developed an Artificial Intelligence (AI) system which can identify people based on partial photos of their faces, through the use of image-matching algorithms. This system matches its images with (leaked) data from government databases which contain photos of various security personnel.

This was widely published in the opposition media channels. Later, they echoed this message



Using image-matching algorithms

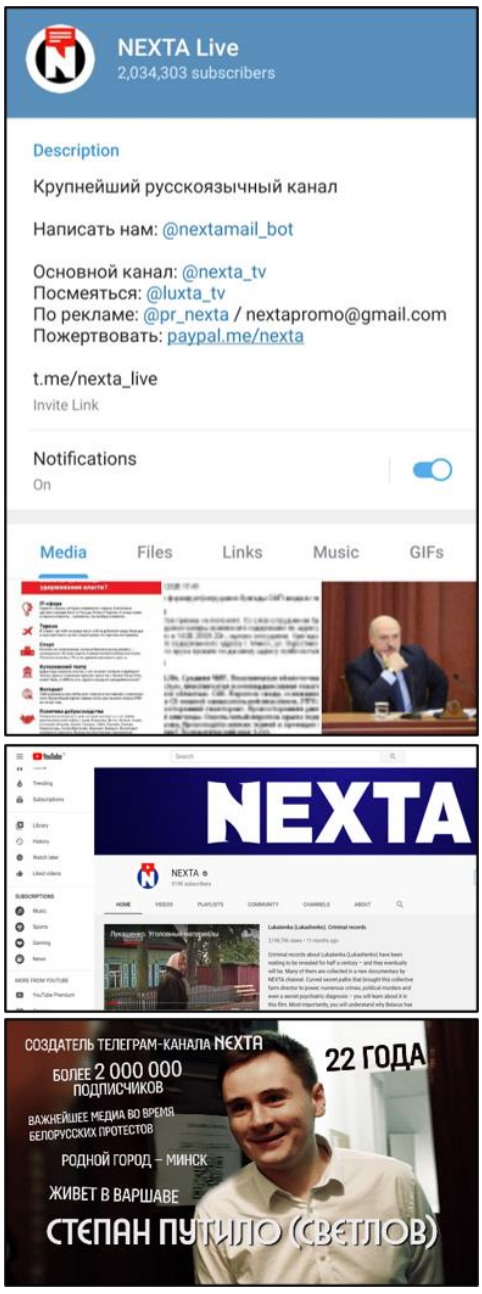


very widely to try and deter security personnel and their families from using violence against protesters.

Using of an independent media channel

The opposition channel NEXTA TV plays an important role in the protests. It's a TV channel broadcasting on Telegram and YouTube. Within a short time, it managed to register over 3 million subscribers. It disseminates opposition messages and calls for a regime change. The main messages include:

1. Showing the violence of the security forces against protesters.
2. Appealing to the security forces to stop their violence, join the protesters and fight the regime.
3. Screening personal stories of security personnel who "switched sides" and joined the opposition.
4. An effort to influence public opinion in Belarus, communities of Belarussians outside the country, NATO states and the USA.



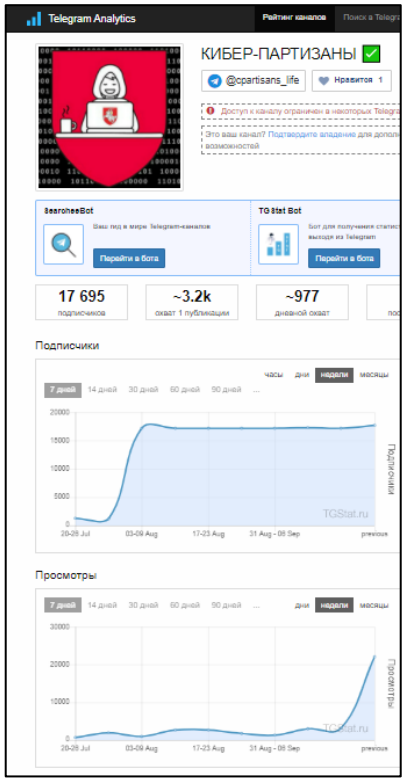
NEXTA LIVE channel

The channel is a stage for opposition leaders to continue their struggle from outside Belarus.

It is interesting that those running the channel are young people (aged 20+) who do it from Poland. The channel organizers encourage users to use VPNs, thereby bypassing some of the country's internet access restrictions.

Managing the protests and communication methods

Despite the large number of protesters, within just a few weeks several hubs have been set to communicate with them all. The main contacts go through Telegram channels, and more sensitive discussions use small chat platforms sometimes built for ad hoc purposes. The platforms used are Mastodon and Element.



For geographical management, people widely use Google Maps and other GIS platforms. VPNs such as TOR and encrypted email services are widely used.

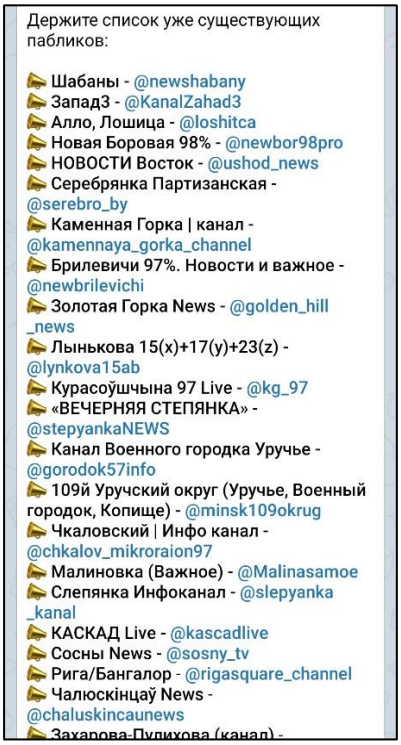
Telegram channels are used to distribute content, documentation and messaging, as well as for organizational purposes. Not surprisingly, another heavily used platform is YouTube.

The opposition is using a website which exploits infographic technology to publicly follow the arrests of protest leaders.

An interesting example of messaging and contacting the public could be seen in the hacking of an invoicing system to distribute messages to people through the printing of legit sales invoices.

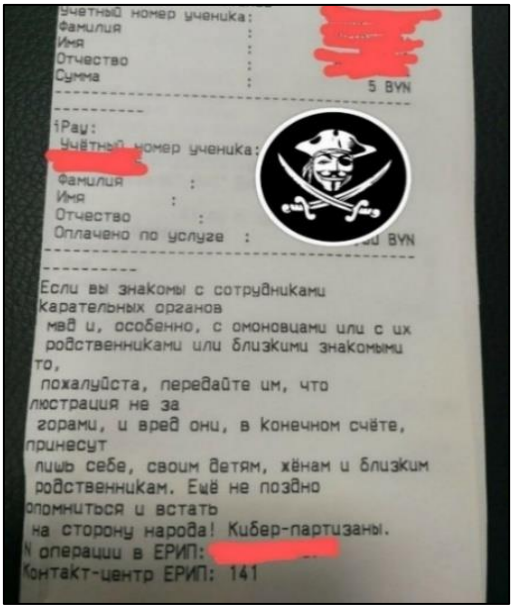
MESSENGER	FOSS	ЦЕНТРАЛИЗАЦИЯ	АНОНИМНОСТЬ	E2EE	СИНХРОНИЗАЦИЯ E2EE	ПРОВЕРКА ОТПЕЧАТКОВ	ЗАПРЕТ НА СКРИНШОТЫ	ГРУППОВЫЕ E2EE-ЧАТЫ	УВЕДОМЛЕНИЕ О ПРОВЕРКЕ E2EE	ЗАЩИТА СОЦ ГРАФА	SCORE
Telegram	Нет	Централизованный	Нет	По выбору	Нет	Нет	Есть	Нет	Нет	Нет	1.5
Signal	Да	Централизованный	Нет	По умолчанию	Есть	Нет	Есть	Есть	Нет	Есть	6
Viber	Нет	Централизованный	Нет	По выбору	Нет	Нет	Есть	Есть	Нет	Нет	2.5
WhatsApp	Нет	Централизованный	Нет	По умолчанию	Есть	Нет	Нет	Есть	Нет	Нет	3
Briar	Да	Децентрализованный	Есть	По умолчанию	Нет	Есть	Есть	Есть	Есть	Есть	9
TamTam	Нет	Централизованный	Есть	Нет	Нет	Нет	Нет	Нет	Нет	Нет	1
Вконтакте	Нет	Централизованный	Нет	Нет	Нет	Нет	Нет	Нет	Нет	Нет	0
Facebook Messenger	Нет	Централизованный	Есть	По выбору	Нет	Нет	Нет	Нет	Нет	Нет	1.5
Wire	Да	Централизованный	Есть	По умолчанию	Есть	Нет	Нет	Есть	Есть	Есть	7
Jabber	Да	Федеративный	Есть	Плагин	Есть	Нет	Нет	Есть	Нет	Нет	5
Riot Matrix	Да	Федеративный	Есть	По выбору	Есть	Есть	Нет	Есть	Есть	Есть	8
Status	Да	Децентрализованный	Есть	По умолчанию	Частично	Есть	Нет	Нет	Нет	Есть	6.5
Threema	Нет	Централизованный	Есть	По умолчанию	Нет	Есть	Нет	Есть	Есть	Есть	6

Comparison between different types of platforms


Держите список уже существующих пабликов:

Шабаны - @newshabany
Запад3 - @KanalZahad3
Алло, Лошица - @loshitca
Новая Боровая 98% - @newbor98pro
НОВОСТИ Восток - @ushod_news
Серебрянка Партизанская - @serebro_by
Каменная Горка | канал - @kamennaya_gorka_channel
Брилевичи 97%. Новости и важное - @newbrilevichi
Золотая Горка News - @golden_hill_news
Лынькова 15(х)+17(у)+23(z) - @lynkova15ab
Курасоўшчына 97 Live - @kg_97
«ВЕЧЕРНЯЯ СТЕПЯНКА» - @stepyankaNEWS
Канал Военного городка Уручье - @gorodok57info
109й Уручский округ (Уручье, Военный городок, Копище) - @minsk109okrug
Чкаловский | Инфо канал - @chkalov_mikroraion97
Малиновка (Важное) - @Malinasamoe
Слепянка Инфоканал - @slepyanka_kanal
КАСКАД Live - @kascadlive
Сосны News - @sosny_tv
Рига/Бангалор - @rigasquare_channel
Чалюскінцаў News - @chaluskincaunews
Захарова-Пудихова (канал) -

Telegram channels by neighborhoods



Transmitting messages based on in-store invoices

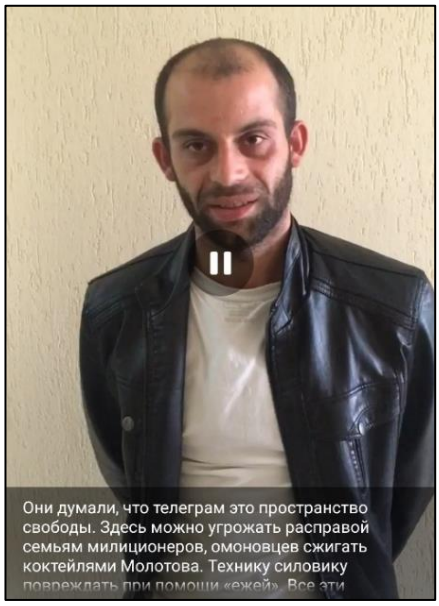
Tracking real-time arrests based by infographic technology

The state's confrontation with the technological struggle

Currently, the administration finds it hard to contest with the "Cyber Partisans". Yet it seems that some actions are taken in various areas:

During the early days of the protests, we saw much activity aimed at restricting internet access in Belarus, including blocking access to social media, email services and various media channels.

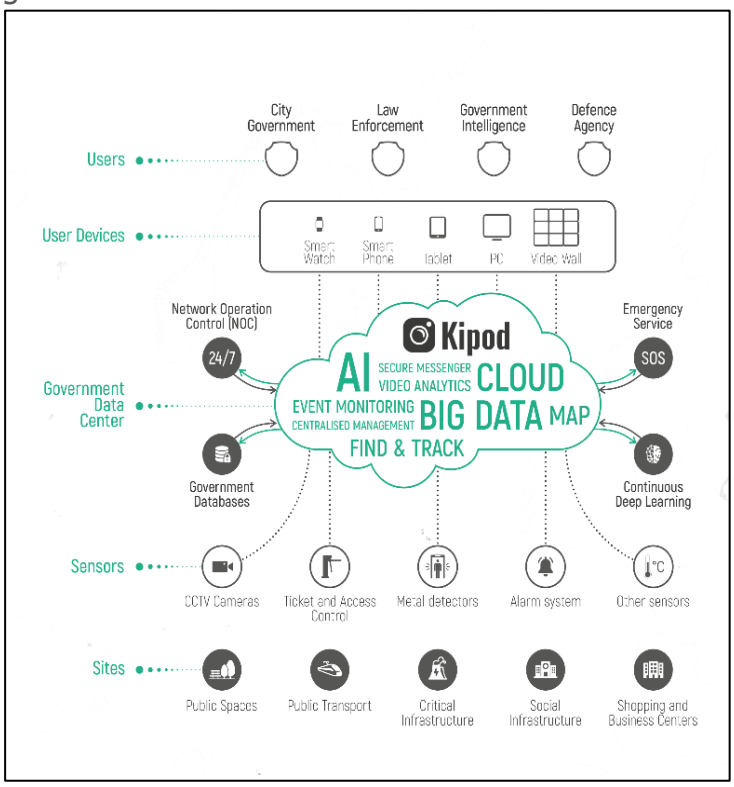
State Incident Response Teams were used to deal with issues in the state's official networks and websites.

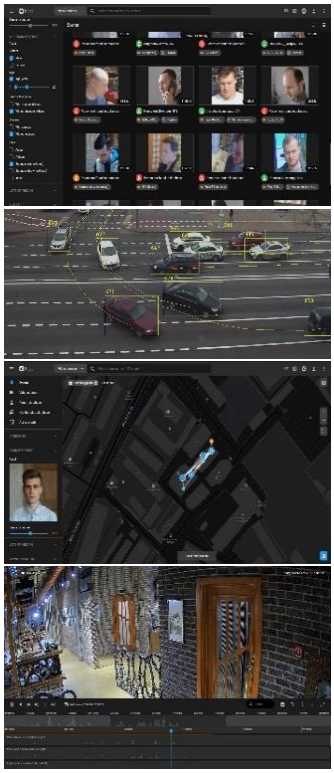


I run this Telegram channel and incited "
"...against the government

Throughout that period, warnings have been published on official websites about cyber attacks and requesting the public to be vigilant against social engineering attempts.

Hurried purchasing and deployment of information security products for government networks.





Exposing the admins who run groups in social media, also in Telegram, and arresting and interrogating them while publishing videos of them repenting and admitting their guilt.

One of the main infrastructures used by the government is a data extraction system called "Kipod" based on big data platforms. This system allows many sensors (street cameras, access control, alarm systems, points of sale and more) to be connected for various purposes: collection, cataloguing and processing data. The system allows real time alerts and searches. It was developed locally and allows a considerable improvement of the activities of the security forces.

Another activity is disarming the legitimacy of cyber attacks (and the protests in general) by insisting that those behind them are foreign countries and interests. In order to raise consciousness, the regime created non-formal media channels for spreading its agenda.

Sending SMS warnings to people informing them that the security forces know of the illegitimate activities and their identities, and would punish them in accordance with the law.

Summary

Despite the fact that the Belarus elections ended on 8 August 2020, it seems they're not over yet. The "Arab Spring" protests that swept the masses through social media and the ability to send real time messages and reports suddenly seems like a "promo" of the massive use of information and cyber technology the protests organizers make in Belarus.

Smartphone – No! Just a simple cell phone

Some of the things described here are not new. Yet one can see new elements of cyber attacks, using technology to enhance the protests, utilizing digital media channels, using open source platforms and utilizing The Wisdom of the Crowds . "Cyber Partisans" is one the most prominent examples. This group uses information technologies and cyber attacks in particular to promote the aims of the protests, while creating a strong psychological linkage to Belarussian heritage and history. Undoubtedly, this is a unique and innovative group that has managed to harness up-to-date technological knowledge for its purposes. When it utilizes cyber technologies in force, with a large scope and diversity, it succeeds, like the old time partisans, in becoming a significant and effective power in Belarus.

In general, one can see how even in this field, technology has a much more central role to play than in the past. At a time when everyone speaks of the influence cyberspace has on society, public opinion and human behavior, this seems to be an intriguing test case.

Only time will tell how this is going to affect Lukashenko's rule.

References

Warning – some of the references below are **active contact channels** of opposition activists in a state whose regime is fighting for its survival. Please avoid/take extra care entering these sources through the links provided.

Official websites:

1. https://www.belarus.by/en
2. https://www.mvd.gov.by/
3. http://www.president.gov.by/
4. https://pravo.by/

Telegram channels:

1. https://t.me/cyberpartisan
2. https://t.me/nexta_live
3. https://t.me/pramenby
4. https://umap.openstreetmap.fr/en/map/map_499264#7/53.566/27.411
5. https://t.me/anarchy_by

YouTube:

1. https://www.youtube.com/watch?v=jrOxsjdeccw
2. https://www.youtube.com/watch?v=O0psTPdWyrQ&feature=youtu.be
3. https://www.youtube.com/watch?v=ArKeFsY94xM&feature=youtu.be
4. https://www.youtube.com/watch?v=FAJIrnphTFg&feature=youtu.be

5. https://www.youtube.com/watch?v=xH9SzfHu8yE

6. https://www.youtube.com/watch?v=R5UmsPFMUaw

7. https://www.youtube.com/watch?v=qcPpPqtX7vs

News sites:

1. https://grodno24.com/2020/09/poslanie-kiber-partizan-na-chekah.html

2. https://regnum.ru/news/polit/3068363.html

3. https://www.pravda.com.ua/rus/news/2020/09/26/7267842/

4. https://www.ferra.ru/amp/news/techlife/belorusskie-kiber-partizany-vzlomali-saity-goskanalov-i-pokazali-po-nim-video-protestov-27-09-2020.htm

5. https://tjournal.ru/news/210962-telegram-kanal-nexta-prigrozil-opublikovat-bazu-dannyh-deystvuyushchih-sotrudnikov-mvd-belorussii-esli-te-ne-ostepenyatsya

6. https://meduza.io/news/2020/09/04/sayt-mvd-belarusi-vzlomali-i-dobavili-lukashenko-v-spisok-razyskivaemyh

7. https://chronicle.znaj.ua/ru/340013-biloruski-kiber-partizani-protestuyut-z-domu-zlamali-kanali-lukashenka-i-pokazali-kadri-pobittiv

Other sites:

1. https://tgstat.ru/channel/@cpartisans_life

2. https://netblocks.org/reports/internet-disruption-hits-belarus-on-election-day-YAE2jKB3

3. https://minsk.sous-surveillance.net/

4. http://czrt.by/notes/palitviazni-u-belarusi-2020/

5. https://kipod.com/