May 2022

Brief

The War in Cyberspace

Russia's War in Ukraine
Series No. 2

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

| Dmytro Dubov |

While attention has largely been focused on the conventional war in Ukraine, Russia's attack has also included sustained cyber-measures. The first month of active conflict saw three times more cyberattacks against Ukraine's information infrastructure compared to the same period in the previous year.[1]

Russia began to test new methods of cyberattack on Ukraine in 2014. Since then, many critical infrastructure facilities (CIF) have been targeted. The more prominent cyberattacks have included those directed at the Ciscarpathian regional energy company (2015) and the Ministry of Finance and State Treasury (2016), and the widespread NotPetya cryptovirus (2017). Russia considers 'information warfare' to be a combination of cyber activity and information and psychological special operations (IPSO) that is executed continuously but intensified during the active phases of a conflict.

The use of cyberspace actions to precede and accompany physical operations, such as riots, provocations or full-scale military operations was seen in Estonia in 2007, Georgia in 2008, and Ukraine in 2014–15. Russia's 2022 military invasion of Ukraine was preceded and accompanied by:

- Attacks on public registers – databases storing citizens' and government data – to provide a base from which to launch future cyberattacks (14–15 January).[2]
- Preparatory attacks: Distributed Denial-of-Service (DDoS) attacks against public information resources and banking institutions, phishing attacks on government authorities and CIFs, spreading of malware, infiltration and vandalism of public and private networks (14–23 February).[3]
- Cyber activities to support the military campaign: emails and simple notification service messages, cyberattacks against CIFs, defacing websites, DDoS, attempts to access internal information systems (24 February on).

Observations from the Cyber Front

Data on the effectiveness of Russian cyberattacks on Ukrainian facilities is limited. Foreign analysts have claimed that numerous successful attacks took place at the beginning of the war.[4] However, only three major cyber incidents have been confirmed: against Ukrtelecom; against the electronic document management systems of some public authorities such as the Ministry of Foreign Affairs; and against Viasat, a satellite communications provider.[5] In addition, Russia has continued, without success, to cyberattack Starlink, a satellite internet service provider.[6]

Russia did not expect, and was not prepared, to maintain cyber activity for a long period

A few preliminary conclusions may be drawn from Russia's cyber activities since mid-January 2022:

- **Limited methods.** Russia has mainly used standard cyberattack methods, such as DDoS and phishing. Phishing attacks have, in general, been of low quality, suggesting that Russia did not expect, and was not prepared, to maintain cyber activity for a long period. Nonetheless, these limited methods have had some success, and may yet become a threat.
- **Limited impact.** Although CIFs are considered by both Ukrainian and international experts to be priority targets for cyberattacks, there have been no signs of successful attacks against Ukrainian CIFs. This may indicate that Russia has failed to breach CIF systems to any significant extent – any successful breaches would likely have been exploited already.

- **Use of personal data.** Hacking attempts on the private email accounts of Ukrainian soldiers and related individuals, notably those hosted by Ukrainian email services i.ua and meta.ua, were reported on 25 February, apparently enabled by thefts of personal data from public registers. The protection of personal data is a vital issue with broader context. Especially disturbing information related to the Bucha massacre indicates that the Russian invaders possessed detailed personal data of Ukrainians, including address, and social and employment status that was used to find and exterminate people according to specific criteria (e.g., whether they are veterans of the Anti-Terrorist Operation / Joint Forces Operation, volunteers, or cooperating with public authorities).[7]
- **Cooperation between Belarusian and Russian special services.** As of mid-April, Ukrainian experts had detected at least 14 different hacker groups related to the Russian and Belarusian special services.[8] Experts also note that special agencies from the Donetsk People's Republic and Luhansk People's Republic are involved – most likely, units of Russia's special services.

Cyber and IPSO

Russia uses information warfare operations to influence the inhabitants of a particular region or country, to promote chaos, suppress resistance and alter political behaviour. Peacetime operations may be aimed at influencing elections in foreign countries (e.g., the US in 2016) or inducing public chaos for political destabilisation (e.g., in Ukraine at the beginning of the COVID-19 pandemic). In crisis and war, cyber operations tend to become more aggressive and targeted at sabotaging or hacking the websites of media outlets and public institutions to spread fake news.

The most notable mass cyber-campaign of Russia's war in Ukraine was on 16–17 March, when over a dozen Ukrainian information resources were attacked simultaneously. The focus of the attack was the on-air news feed of the TV channel Ukraine 24. The attackers managed to initiate a rumour of an address by President Zelensky announcing Ukraine's capitulation, while simultaneously, launching a (extremely low-quality) deepfake of this alleged speech on social media.[9] Hackers also attacked a large number of Ukrainian media websites, exploiting vulnerabilities in the Redtram advertisement app.[10] And on 17 March, more than ten websites reported hackers' attempts to put up web banners with the Russian flag, St George ribbon, "Z" and "V" symbols, etc.[11]

Other websites have also been hacked with the aim of causing chaos and panic. For instance, a number of local community websites in the Odesa region were hacked on 3 March, with hackers posting a call for Ukrainians to lay down their arms alongside disinformation about the Snake Island attack.[12] On 14 March, Russian hackers infiltrated the Zhytomyr City Council website and placed a message on the home page calling for an immediate evacuation and no resistance to the invaders.[13] This was an almost verbatim repetition of a message left by hackers on the Zaporizhzhia City Council home page (a mention of "Zaporizhzhia City Council" was even left unchanged). On 17 March, they hacked the website of the Ukrainian judiciary to place fake propaganda about Ukrainian defenders, whom they called nationalists, and to accuse them of capturing Ukrainian civilians and using them as human shields.[14]

Russian cyber activity is closely coordinated with the Russian propaganda machine

Most of these breaches were covered by Russian mass media at a speed that suggested they were either coordinated directly with Russian mass media representatives or reported immediately afterwards for prompt coverage. Such tactics are not new to Russian hacker groups. For example, in Ukraine's 2014 Presidential election, Russian hackers failed in their planned attack to manipulate data on the Central Election Commission website, but Russian TV still broadcast the false data. Russian cyber activity is thus closely coordinated with the Russian propaganda machine: hackers and media managers collaborate on the implementation and prompt reporting of manipulated events.

Future challenges for Russia

While the war is far from over, it is apparent that Ukraine's efforts to maintain cybersecurity have so far been a considerable success. Ukraine has prevented any failure of its vital IT systems and Ukrainian and foreign cyber activists have successfully counter-attacked a range of targets inside Russian territory. For example, data from numerous Russian companies and organisations (including the personal data of Russian military personnel involved in the war) have been obtained.

Major websites of Russian governmental and public institutions have been temporarily taken down, using tools rapidly created at the start of the war by pro-Ukrainian cyber activists that have enabled anyone with a minimum knowledge of cybertech to take part in cyberattacks.

These challenges, and the efforts by many globally to contain Russian cyber threats, indicate that Russia will face several long-term challenges to its cybersecurity and cyberwarfare capabilities:

- **Shortage of specialists.** Russia's best specialists (including those dealing with cybercrimes) have been involved in offensive cyber activities, but the increasing number of cyberattacks against Russian infrastructure will force them to focus on defence, decreasing their offensive potential.
- **Limited awareness of cybersecurity.** The cyberattack on the Russian Air Transport Agency is a prominent example of the lack of awareness of the need for strong cybersecurity - there were no backups from which to restore governmental email and e-document management services. Successful cyberattacks on the websites of the Russian government, president, public and security services, and central bank have shown that despite attention to, and public funding of, cybersecurity, the abilities of Russian cybersecurity specialists tend to be limited.

Russia's responses in the current cyber conflict have been poorly thought out

- **Weak operational skills of mid-level specialists.** Despite their high reputation, Russian hackers (and IT specialists in general) have failed to show their supposed mastery in this active cyber confrontation. In the past, successful operations have usually had an elaborate action plan and detailed target list. Russia's responses in the current cyber conflict have been poorly thought out and its cyberattacks against Ukraine have been partly supported by data gathered by Russian intelligence agencies through traditional means such as human espionage.[15]
- **Withdrawal of foreign expertise.** Nearly 40 cybersecurity companies have announced their withdrawal from the Russian market and have suspended service for Russian clients.[16] This presents long-term challenges, as many software or hardware solutions cannot be replaced by Russian-owned technologies (according to Russian specialists, replacement may require 6 to 12 months). Meanwhile, a Presidential Decree of 30 March 2022 required all purchases of foreign software for Russian CIFs to be suspended from 31 March and prohibited the use of foreign software from 1 January 2025.[17] Further, by the end of September 2022, the Russian government must develop a plan to replace foreign-made radio, electronic and telecommunication devices with Russian ones. This might be impossible, according to some assessments, as available Russian technologies are significantly inferior to their foreign equivalents. In any event, a ban on importing technologies will be a sham, as it will only make the existing practice of purchasing Chinese products and replacing "made in China" labels with "from Russian manufacturers" even more widespread.[18]
- **Brain drain.** Another long-term challenge is that many Russian cybersecurity specialists (perhaps even a quarter) are planning to leave Russia. The Russian government will need to find solutions, which are likely to be further restrictions rather than incentives. On 25 March 2022, a media article reported that a Concord group company associated with Yevgeny Prigozhin (an oligarch close to Putin) had urged the government to draft a law to make it harder for IT specialists to travel abroad.[19] Both the Russian Ministry of Digital Development and Kremlin spokesman Dmitry Peskov later denied this, and the information was deleted.[20] Separately, State Duma member Alexander Khinshtein suggested establishing 'IT-joints', similar to the Soviet-era semi-prisons where sentenced specialists worked on R&D projects, supervised by the security service.[21] It seems that this was not a serious proposal, but as many Russian IT specialists have been arrested recently, it may have been a trial balloon intended to test the idea and to mentally prepare the Russian public.

Unless addressed, these challenges will degrade Russia's ability to compete in the highly dynamic sphere of cyberspace – even as the war in Ukraine has shown the extent of its failures to deliver effects in this domain too.

Endnotes

1 Державна служба спеціального зв›язку та захисту інформації України [State Service of Special Communication and Information Protection of Ukraine], "За місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року [During one month of war, there have been almost three times as many hacker attacks as during the same time period last year]," Facebook, 3 April 2022.

2 "Від кібератаки 14 січня постраждали 22 державних органи Держспецзв'язку [The cyberattack on January 14th affected 22 state bodies of the Special Service]," Cabinet of Ministers of Ukraine, 25 January 2022.

3 Державна служба спеціального зв'язку та захисту інформації України [State Service of Special Communication and Information Protection of Ukraine], "Сайти низки державних та банківських установ знову зазнали масованої DDoS-атаки [The sites of several government and banking institutions have once again undergone a massive DDoS attack]," Facebook, 23 February 2022.

4 David Cattler and Daniel Black, "The Myth of the Missing Cyberwar," *Foreign Affairs*, 6 April 2022.

5 Sean Brian Townsend, "Я так понимаю, что по части кибервойны аналитики ждали нечто среднее между "Die Hard 4" и нашествием Гая Фокса [I understand that in terms of cyberwarfare, analysts were expecting something in between "Die Hard 4" and Guy Fawkes' invasion]," Facebook, 6 April 2022; Gordon Corera, "Russia hacked Ukrainian satellite communications, officials believe," *BBC*, 25 March 2022.

6 Ivan Maguryak, "Російські хакери намагаються атакувати супутникові термінали Starlink в Україні [Russian hackers are trying to attack Starlink satellite terminals in Ukraine]," *Kanal24*, 26 March 2022.

7 Политика Страны (@stranaua), "Секретарь Бучанского городского совета Тарас Шаправский в комментарии "Стране" рассказал о ситуации в городе [In a commentary to "Strana", secretary of the city council of Bucha, Taras Shapravsky spoke about the situation in the city]," Telegram, 3 April 2022; Olga Kipilenko, "Диявол носить форму російського солдата. Як катували на Київщині [The devil wears the uniform of a Russian Soldier. How they tortured people in the Kyiv region]," *Українська правда*, 6 April 2022.

8 "Хто стоїть за кібератаками на українську критичну інформаційну інфраструктуру: статистика 15–22 березня [Who is behind cyberattacks on Ukraine's critical information infrastructure: statistics from March 15 to 22]," *056.ua* (Site of the Dnieper), 26 March 2022.

9 Хакери зламали стрічку в ефірі "Україна 24" та оприлюднили фейк про "капітуляцію Зеленського" [Hackers broke the news feed of "Ukraine24" and published fake news about "Zelensky's capitulation"]," *DM Media Sapiens*, 16 March 2022; Taras Mishchenko, "Рашисти намагаються запустити діпфейк з Зеленським, але навіть його не спромоглися зробити [Racists are trying to launch a deepfake with Zelensky, but they have not achieved even that]," *Mezha Media*, 16 March 2022.

10 Kostia Andreikovets, "Russian hackers are trying to hack the Ukrainian media through the Redtram application," *Babel,* 26 March 2022.

11 "Хакери атакували українські новинні сайти. Намагалися почепити банер із георгіївською стрічкою [Hackers attacked Ukrainian news sites. They tried to create banners with the ribbon of Saint George]," *Detektor Media*, 17 March 2022.

12 Tamara Gladka, "На Одещині російські хакери зламали сайти усіх територіальних громад [In the Odessa region, Russian hackers hacked the sites of all local communities]," *Новое Время*, 3 March 2022.

13 Alina Tys, ""Шановні житомирці...": російські хакери зламали сайт Житомирської облради ["Dear citizens of Zhytomyr...": Russian hackers hacked the website of the Zhytomyr Regional Council]," *Radio Trek*, 14 March 2022.

14 Anastasia Kushpit, "Росіяни зламали суддівські сайти та помістили туди пропаганду [Russians hacked court websites and posted propaganda]," *24Kanal*, 17 March 2022.

15 Державна служба спеціального зв›язку та захисту інформації України [State Service of Special Communication and Information Protection of Ukraine], "Серед російських хакерів, які атакують українські державні інформаційні ресурси та критичну інформаційну інфраструктуру, є дві групи [There are two groups among Russian hackers attacking Ukrainian state intelligence resources and critical information infrastructure]," Facebook, 27 March 2022.

16 Alexey Lukatsky, "Какие зарубежные ИБ-компании приостановили бизнес в России? [Which foreign information security companies have suspended their business in Russia?]," *Aleksey Lukatsky's site on cybersecurity* (blog), 15 March 2022.

17 "Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" [Decree of the President of the Russian Federation on 30 March 2022 No 166 "On Measures to Ensure the Technological Independence and Security of Critical Information Infrastructure in the Russian Federation"]," The official Internet portal of legal information of Russian Federation, 30 March 2022.

18 ""Привыкли, что ничего работоспособного в стране нет": как в России годами пытаются "победить" Intel, Huawei и Dell ["We are used to nothing working in the country": how they have been trying to "defeat" Intel, Huawei and Dell in Russia for years]," *TJournal* (blog), 21 January 2021.

19 "В России предложили усложнить выезд IT-специалистов за границу [Russia has proposed to make it difficult for IT specialists to travel abroad]," *iXBT.com*, 25 March 2022.

20 "Песков назвал "уткой" сообщения об ограничениях на выезд из России IT-специалистов [Peskov called the reports of restrictions on the departure of IT specialists from Russia a rumor]," *SecurityLab.ru*, 25 March 2022.

21 "Хинштейн пошутил про создание "шарашек" для осужденных айтишников [Khinshtein joked about setting up "sharashka" for convicted IT specialists]," *Interfax*, 22 March 2022.

About the Author

Dmytro Dubov

Dr. Dmytro Dubov is Head of the Information Security and Cybersecurity Department of the National Institute for Strategic Studies in Kyiv, Ukraine. He is also a contributing expert of Resilient Ukraine programme of ICDS.

ICDS.Tallinn
@ICDS _ Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076