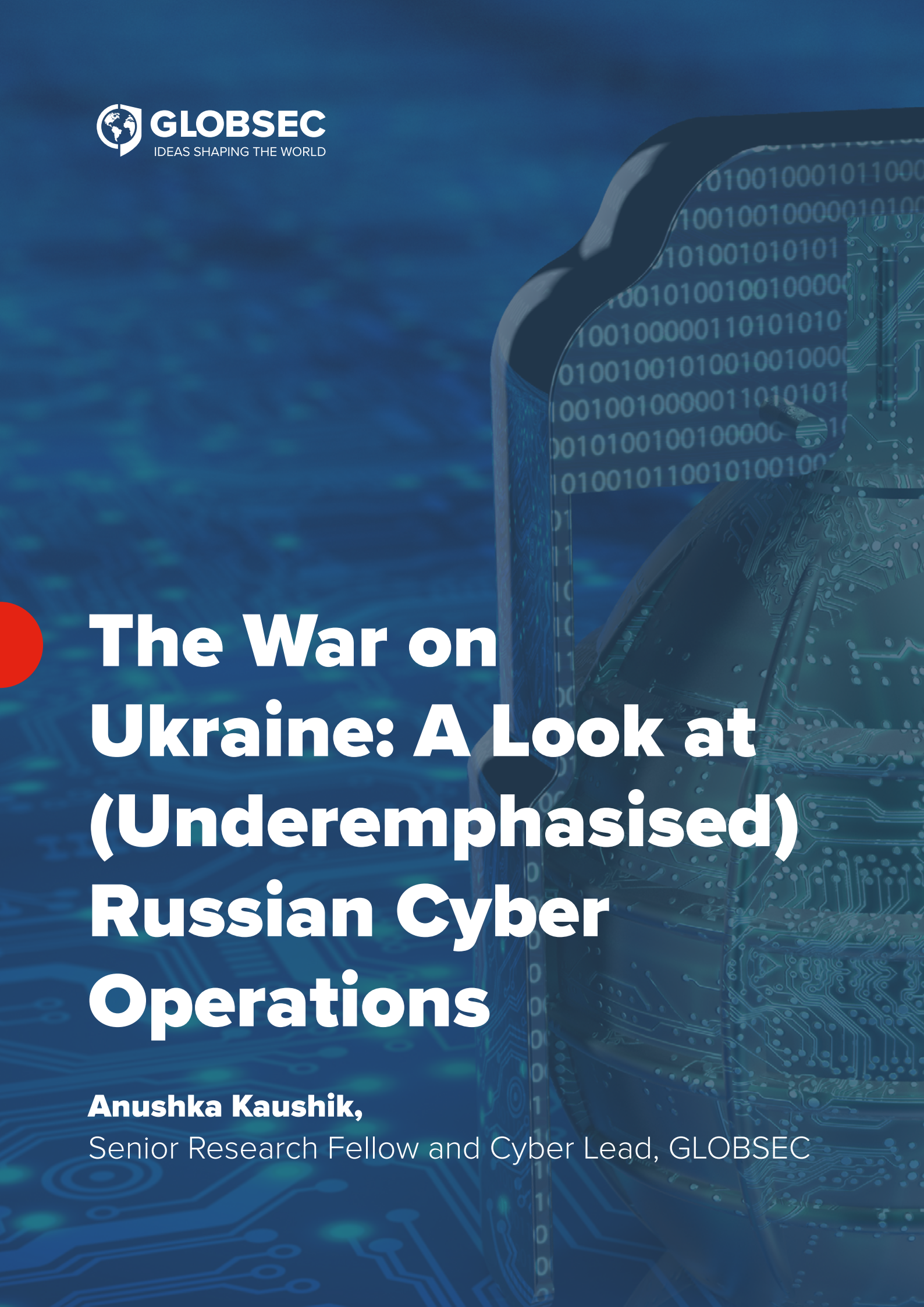
GLOBSEC
IDEAS SHAPING THE WORLD



The War on Ukraine: A Look at (Underemphasised) Russian Cyber Operations

Anushka Kaushik,
Senior Research Fellow and Cyber Lead, GLOBSEC

This brief is published under the aegis of the GLOBSEC Future of Cyberspace Initiative: Transatlantic Chapter. This initiative aims to carry out in-depth assessments of the Transatlantic partnership, the Pan-European partnership, and the Central and Eastern European partnership in the field of cybersecurity with the goal of providing implementable roadmaps to strengthen the overall cybersecurity posture.

Executive summary

February 24, 2023 will mark one year of Russia's invasion of Ukraine with no signs suggesting the end of the war is near. The threat of escalations in cyberspace by Russian actors looms large for Ukraine even as its increased preparedness has allowed it to thwart multiple attacks. For Transatlantic governments, it is equally important to analyse Russian cyber intrusions of the past year as it is to defend against future attacks. Despite the consistent pace of cyber-attacks by Russia, there has been a lack of emphasis on the role of cyber operations since the invasion. While combined efforts towards Ukraine's cyber readiness have borne results and prevented further escalations, narratives around the existing level of cyber operations in the war preliminarily indicate a misunderstanding of the scope and nature of how conflict can play out in cyberspace. This can have deleterious consequences for policy and strategy planning. This brief aims to highlight Russian cyber operations since its invasion, including some noteworthy trends and identified priorities for governments and policymakers to address in the immediate future. It also touches upon the transnational efforts to pushback against Russia and elaborates on Ukraine's enhanced cyber defence with contributions from the private sector and the European Union, United States, and North Atlantic Treaty Organisation (NATO).

Russia's cyber operations since the invasion

Russian threat actors – both known and with suspected links to the government – have been carrying out a combination of cyber-attacks including deploying destructive malware and espionage activities since the invasion of Ukraine on February 24, 2022. These include Distributed Denial of Service (DDoS) attacks, wiper malware, faux ransomware (i.e. destructive malware designed to look like ransomware with the goal of making targeted devices inoperable), information stealers among others. Of note is destructive malware Industroyer 2 – identified by Bratislava-headquartered cybersecurity company ESET which worked with CERT-UA to take remedial action against it thereby protecting a high-voltage electrical substation[1]. ESET and CERT-UA's collaboration also indicated that this is a new version of Industroyer used in the notorious 2016 Ukrainian electric grid attack that left thousands without electricity.

The intended effects of cyber-attacks have been far reaching across Ukraine – ranging from hampering communications, preventing distribution of relief supplies, restricting access to government websites, inhibiting public access to information, and disrupting reliable internet connectivity.

Publicly available data suggests that between July to September 2022, there was a 248% increase in incidents in Ukraine compared to previous quarters with public administration being the most targeted sector[2]. While the target has primarily been the public administration sector, Russian actors have also targeted private satellite infrastructure, media entities, cryptocurrency platforms, and NGOs. Critical infrastructure (CI) has been a consistent target of cyber-attacks with more than 40% of destructive attacks aimed at organisation in CI sectors with the element of securing access to CI for future destruction predating the conflict[3]. There is also technical evidence that indicates attempts to gain access to networks was done as early as December 2021[4].

Industroyer 2 deployed against Ukrainian high-voltage electrical substation in April 2022

According to ESET research, this was a new variant of Industroyer malware used in 2016 to cut power in Ukraine

Campaigns that were attributed to Russian state-sponsored threat actors including those from Gamaredon aka Primitive Bear – attributed to Russia's Federal Security Services, Turla – attributed to Russia's Federal Security Service, Sandworm – attributed to Russia's foreign military intelligence (GRU) among others[5]. In some cases, like the malware attack against communications giant Viasat, technical attribution has accompanied political attribution – by the Council of the EU, the United Kingdom, and U.S. Intelligence. For most of the incidents, there have been technical attributions by the private sector or technical and political attributions by CERT-UA, although Western governments have publicly denounced Russian activity in cyberspace, as have the various bodies of the European Union.

1 ESET Research, Industroyer 2: Industroyer Reloaded, *We Live Security* (12 April 2022), https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ , accessed 5 January 2023

2 The Cyberpeace Institute, 'Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q3 July to September 2022', *Cyberpeace Institute* (16 December 2022) https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/, accessed 5 January 2023

3 Microsoft, Special Report: Ukraine, An Overview of Russia's Cyberactivity in Ukraine, *Microsoft* (27 April 2022) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd , accessed 6 January 2023

4 Threat Hunter Team Symantec, Ukraine: Disk-wiping Attacks Precede Russian Invasion, *Symantec Enterprise Blogs/Threat Intelligence* [blog post] (24 February 2022), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia, accessed 8 January 2023

5 The Cyberpeace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q3 July to September 2022', *Cyberpeace Institute* (16 December 2022) https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/, accessed 5 January 2023

Some noteworthy trends

1. There has been consistency in cyber-attacks by Russian-affiliated groups since the invasion.

According to industry data and expert interviews, the operational tempo of cyber-attacks has been high and at a consistent pace with most of the activity coming from GRU-affiliated actors[6]. Several industry sources indicate that the since the beginning of the invasion, destructive wiper malware has been deployed multiple times a week with the aim of destroying files of multiple organisations in Ukraine.

2. There is preliminary evidence that cyber-attacks have complemented kinetic warfare.

Almost one year into the war, there are indications that a portion of the kinetic attacks were in concert with attempted cyber intrusions. Microsoft reports suggest that from the start of the invasion through April 2022, Russian cyber and kinetic military operations appeared to be conducted with similar objectives, targeting the same sectors or geographic locations – indicating that in some cases, high concentration of malicious network activity overlapped with high intensity fighting[7]. The Ukrainian State Special Intelligence Service and the Ukrainian Economic Security Council published a study in January 2023 mapping Russian strategies since the invasion, indicating that there has been a widespread coordination of attacks in different dimensions[8].

3. There is increased activity from hacktivists on both sides.

An early notable example is of the Ukrainian nuclear agency Energoatom which reported a Russian cyber-attack against its website in August, attributing it to the People's Cyber Army hacker group. More recently in November 2022, the European Parliament's website suffered a DDoS attack after European lawmakers labeled Russia a state sponsor of terrorism, which pro-Russian hacktivist group Killnet took responsibility for[9].

While hacktivism is not new in a country with a tradition of patriotic hackers, there are several factors that could have contributed to the increased intensity of this activity during the war. Increased media coverage of Russian hacktivist collectives and their consequent portrayal as patriots and defenders enhanced the spotlight on hacktivist activities. The establishing of the IT Army of Ukraine could have also spurred activity on the Russian side to retaliate. Killnet has claimed to carry out DDoS attacks against US airports, the White House, StarLink, various websites of European government websites, among others. It is important to mention however that the primary tool for hacktivist groups like Killnet have been DDoS attacks which have had limited effects, necessitating a much closer look at the scope, and intended effects of third parties in cyber conflict.

4. There is growing involvement of established Russian cybercrime groups.

In addition to exploiting the war for person financial gains, established cybercrime groups are also aiding Russia's policy objectives by publicly pledging support to the Russian people and government. This has extended to open threats to conduct cyber operations to retaliate against perceived attacks against Russia or resource support for Ukraine. These include Salty Spider, Scully Spider, Smokey Spider, The Cooming Project among others[10].

---

6 J. Wolfram, G. Roncone, T. McLellan, interview with L. McNamara, 'Threat Trends: Reflections on Russian Cyber Threat Activity During the War in Ukraine ', *The Defender's Advantage Podcast*, (23 November 2022), Mandiant, https://www.mandiant.com/resources/podcasts/threat-trends-russian-threat-activity-ukraine, accessed 4 January 2023

7 Microsoft, Special Report: Ukraine, An Overview of Russia's Cyberactivity in Ukraine, *Microsoft* (27 April 2022) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd , accessed 6 January 2023

8 I. Khemlova, Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions, *State Service of Special Communications and Information Protection of Ukraine,* (17 January 2023) https://cip.gov.ua/ua/news/doslidzhennya-zv-yazok-mizh-kiberatakami-konvenciinimi-ta-informaciinimi-atakami-v-ukrayini-vidpovidaye-rosiiskii-koncepciyi-gibridnoyi-viini , accessed 21 January 2023

9 M. Burgess, 'Hacktivism is Back and Messier Than Ever', *Wired* (27 November 2022) , https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos, accessed 3 January 2023

10 Canadian Centre for Cybersecurity, Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine, *Canadian Centre for Cybersecurity Centre,* (14 July 2022), https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine , accessed 4 January 2023

5. There is evidence of cyber-attacks beyond Ukraine, against European and American networks.

Both government and industry data have indicated increased cyber espionage efforts from Russian state-sponsored threat actors targeting the United States and European countries in response to its support for Ukraine – indicating that while kinetic combat has not been directed at NATO countries, cyberspace for that purpose is already being used.

In Central and Eastern Europe, DDoS attacks against government websites have been frequent, targeting multiple sectors of critical infrastructure including Romania, Slovakia, and the Czech Republic[11]. In early April, Ukrainian authorities publicly reported several spear-phishing attempts targeting certain European government targets, attributed to the FSB[12]. The destruction caused by NotPetya in 2017 is also a reminder of the danger of spill-off effects from Russian cyber-attacks – this has already been witnessed since the invasion when Viasat's European KA-SAT satellite communications service network was disrupted by Russian actors. This led to thousands of KA-SAT satellite network modem being rendered inoperable, including in in France, Germany, Greece, Hungary, Italy, and Poland. More recently, Prestige ransomware – attributed to Russian threat actor IRIDIUM – has affected networks of organisations in transport and logistics in Ukraine and Poland[13].

6. There has been an underestimation of the level of cyber operations.

Russian actors have used over forty destructive malware, espionage attacks, and targeted critical infrastructure at a high operational pace. However, the dominant narrative in defence strategy and policy circles has pointed to a subdued role of cyber tools as against the expectation of cyber operations dominating and playing a decisive role in the conflict.

This misrepresentation can have deleterious consequences for strategic planning and can lead to a general underestimation of threats emerging from cyberspace, at a time when it is critical for national security doctrines to continue addressing cyber risks. With increased attacks against critical infrastructure like the Colonial Pipeline incident in 2021 even before the war and the unprecedented numbers of ransomware attacks globally, underestimating cyber threats can have far-reaching consequences.

There are numerous indications that the efforts to make cyber a domain of conflict by Russian actors in this war exist – by the consistent operational pace of cyber-attacks, by critical infrastructure as intended targets for a host of attacks, by the possible complementarities between kinetic and cyber-attacks, and by the targeting of networks of NATO countries. The underestimation of cyber operations in the conflict has also partly been due to the hyperbole of their effects and scope – narratives and expectations of Cyber Armageddon and Cyber Pearl Harbour are largely unproductive and lend toward an unhelpful assessment in escalating conflict. Mischaracterizing cyber weapons/strikes as tools that function with the same speed and efficiency as kinetic ones or conflating cyber and kinetic capabilities in conflict to have identical effects may have contributed toward certain predictions of what a cyberwar may look like.

Seeing Russia's aggressive and malicious behaviour in cyberspace as an intensification of their pre-war activities offers a more realistic picture – bearing in mind that as risks of escalation in cyberspace increase, Western partners will need to address more fundamental questions on how they would choose to respond and where they would draw the lines. The role of cyber operations in this conflict, thus, necessitates a deeper examination of several questions that could shape our strategies on the use of cyber tools in warfare – such as the role of third parties in conflict like hacktivist groups on both sides, persisting definitional challenges of 'cyber war' and applicability of Article 51, utility of cyber operations in kinetic conflict among others.

11 T. McEnchroe , Interior Minister: Russia behind cyber-attack on Czech institutions, *Radio Prague International* (21 April 2022) https://english.radio.cz/interior-minister-russia-behind-cyber-attack-czech-institutions-8748268 , accessed 8 January 2023

12 Canadian Centre for Cybersecurity, Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine, *Canadian Centre for Cybersecurity Centre,* (14 July 2022), https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine , accessed 4 January 2023

13 Microsoft Security Threat Intelligence, New 'Prestige' Ransomware Impacts Organizations in Ukraine and Poland, *Microsoft Security* [blog post] (14 October 2022), https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ , accessed 10 January 2023

Suggested priority areas for 2023.

1. Specific elements of critical infrastructure in the **energy and financial sectors** are particularly vulnerable targets for Russia's cyber operations – there is already increasing evidence of broad-based targeting of energy facilities against Western countries.

2. With concrete steps of Western unanimity against Russia comes the very real threat of escalation in cyberspace. This also extends to **infrastructure in space** such as Starlink – which with the help of USAID has contributed significant resources to Ukraine – that is facing an increasing number of cyber-attacks from Russian threat actors[14].

3. **Increasing accountability** of actors like Russia through **more coordinated political attributions** and diplomatic measures will be required as norms of acceptable behaviour in cyberspace continue to be violated despite consensus on the UN GGE resolution in 2021.

4. **Enhancing existing mechanisms** like the EU Cyber Diplomacy Toolbox to also address the incremental increases in malicious behaviour in cyberspace as opposed to a defined incident threshold can be an example.

5. The EU and the US can start working towards a **more operational approach to cyber defence** with the involvement of the private sector. EU's Cyber Defence Policy (presented on Nov 10)[15] in response to rising geopolitical tensions, called on Member States to increase investments in modern military cyber defense capabilities, making a reference to the importance of active cyber defence. Even as the concrete aspects of the policy will take time to shape due to the involvement of the Member-States, defining a common doctrine of defending forward and the scope of offensive cyber capabilities.

6. **Closer examination of the role of the private sector** in the conflict with a view to enhancing day-to-day operational collaboration between the public and the private sector can prove to be beneficial. Given that significant data and capabilities vest within the private sector, governments must work on ways to leverage that, and the role played by companies in the Russian-Ukraine war provides a possible roadmap.

14 K. Duffy, A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine, *Business Insider* (22 April 2022), https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4 , accessed 3 January 2023

15 European Commission Press Release, 'Cyber Defence: EU boosts action cyber threats', *European Commission* (10 November 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642 accessed 5 January 2022

A short note on the combined efforts toward Ukraine's cyber defences

Definitional challenges around 'cyber war' aside, Ukraine's enhanced preparedness has played a key role in limiting the effects of Russia's cyber operations. The Security Service of Ukraine (SSU) has been at the forefront of the effort to shore up Ukraine's cyber defences since before the Russian invasion – including implementing a Malware Information Sharing system (MISP-UA) based on open-source software, taking inspiration from EU and NATO best practices in 2018 and making continuous updates[16].

Having been a victim of significant destructive attacks by Russia for quite some time now – including the 2016 electric grid attack and the devastating NotPetya ransomware – Ukraine's security service has been scaling efforts in prevention, detection, and neutralizing attacks which has extended to conducting active counteroffensive operations in the cyber domain.

A few days before the invasion, on Feb 17, 2022, Ukraine authorities authorized migrating national data to the public cloud from servers operating entirely within the country. This move was significant as it enabled critical protection of data and is indicative of Ukraine's prioritizing of cyber resilience – while defenses might be overcome, having a backup for critical data that is separate can offset the consequences of an attack.

Furthermore, the early success of a transnational effort to pushback against Russia is indicative of the level of cooperation forged between Ukraine and the European Union, United States and other NATO countries on cyber resilience. The joint response of the EU and US to Russia's aggression in cyberspace has been swift, mirroring their efforts to support Ukraine in all other domains including humanitarian aid, physical resources, and financial assistance. That support has entailed deploying experts to boost Ukrainian cyber defense, donating funds for telecommunications equipment, and facilitating Ukraine's admission in key European institutions as well as NATO centers to bolster their access to critical information.

In March 2022, President von Der Leyen and President Biden's statement of support for Ukraine highlighted advancing cooperation on cybersecurity by supporting Ukraine's cyber resilience, cyber defence, ensuring Internet access for Ukrainian citizens, and working together to reinforce responsible state behaviour in cyberspace[17]. It called for scaling cyber resilience in the face of 'destructive, disruptive, destabilising' cyber-attacks while reiterating the significance of the Counter Ransomware Initiative – an informal platform with 37 countries and 13 companies with the aim of instituting a set of cyber norms recognized across the globe to counter criminal ransomware threats and hold malicious actors accountable. At the NATO Summit held in Madrid in June[18], Allies pledged to improve cyber defences and resilience of Ukraine while expanding partnerships with industry and strengthening cyber defences via enhanced civil-military cooperation.

In July 2022, US' Cybersecurity and Infrastructure Security Agency and Ukraine's State Special Communications Service of Ukraine signed a Memorandum of Cooperation (MoC) to further facilitate information exchanges and sharing of best practices on cyber incidents, technical exchanges on critical infrastructure, and cyber training and joint exercises[19].

Early in the war at Ukraine's request, under EU's Permanent Structured Cooperation structure (PESCO) – representatives from Lithuania, Croatia, Estonia, Netherlands, Poland, and Romania were deployed as part of the Cyber Rapid Response Team (CRRT) to aid Ukraine's cyber defense efforts[20]. This marked the first time that the CRRT was deployed since reaching full operational capability in May 2021. Under the 'EU Support to Strengthen Cybersecurity in Ukraine' implemented by Estonian e-governance Academy, the EU has pledged more than 10 million euros

16 Security Service of Ukraine, 'SBU cyber specialists upgrade MISP-UA platform: to more effectively protect state authorities from hacker attacks', *Security Service of Ukraine* (14 June 2021) https://ssu.gov.ua/en/novyny/kiberfakhivtsi-sbu-onovyly-platformu-mispua-shchob-efektyvnishe-zakhyshchaty-orhany-derzhavnoi-vlady-vid-khakerskykh-atak accessed 4 January 2023

17 The White House, Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement, White House Briefing Room (25 March 2022) https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/, accessed 10 January 2022

18 NATO, Madrid Summit Declaration, *NATO Official Text* (29 June 2022) https://www.nato.int/cps/en/natohq/official_texts_196951.htm , accessed 6 January 2023

19 Cybersecurity and Infrastructure Security Agency, United States and Ukraine expand cooperation on cybersecurity, *Cybersecurity and Infrastructure Security Agency News,* (27 July 2022) https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity , accessed 5 January 2023

20 European Defence Agency, Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, *European Defence Agency News and Events* (24 February 2022), https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence, accessed 11 January 2023

by February 2023 and 15 million euros from the 330 million package to support resilience digital transformation[21]. Concrete steps are also being taken for Ukraine to attain special partner status of the EU's foremost agency on cybersecurity – European Network and Information Security Agency (ENISA)[22].

Therefore, these efforts have been expeditious and wide-ranging, and bode well for future joint responses to bolster cyber defences during conflict. It also builds on existing mechanisms which were a result of some key programs launched before the war.

- **2020**: A 38 million USD cybersecurity reform program under USAID to strengthen Ukraine's cybersecurity legal and regulatory environment and build Ukraine's cyber workforce[23].
- **2019**: The EU4Digital Cybersecurity East Project where the EU seeks to strengthen the protection of critical information infrastructure and increase the operational capacities for cybersecurity incidents management in Eastern European countries including Ukraine[24].
- **2014**: The NATO Trust Fund on Cyber Defence for Ukraine declared operational in 2014, with the aim of providing Ukraine with the necessary support to develop its strictly defensive, CSIRT1 -type technical capabilities, including laboratories to investigate cyber security incidents – managed by the Romanian Intelligence Service as lead partner, the fund stands at a 965K EUR[25].

A noteworthy development in global efforts to support Ukraine's cyber resilience has been the role played by technology companies – highlighting once again how crucial the private sector is in securing cyberspace. Microsoft, for example, aided the Ukrainian government in moving critical government data outside the country and to the public cloud – which was illegal before the war according to Ukrainian data laws – thereby protecting sensitive data and committed a total of $107 million for technology services to support this effort[26]. Free security services were provided by vendors like Google, ESET, Cloudflare, CISCO among others to Ukrainian users and working closely with the Ukrainian government was a collective cyber defense effort rarely seen before.

21 EU4Digital, EU supports cybersecurity in Ukraine with over €10 million, *EU4Digital News,* (21 October 2022) https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/#:~:text=The%20EU%20will%20spend%20more,cybersecurity%20and%20data%20security%20needs. , accessed 10 January 2023

22 State Service of Special Communications and Information Protection of Ukraine, 'Ukraine enhances cooperation with ENISA', *State Service of Special Communications and Information Protection of Ukraine News,* (7 October 2022) https://cip.gov.ua/en/news/ukrayina-rozvivaye-spivpracyu-z-agentstvom-yes-iz-merezhevoyi-ta-informaciinoyi-bezpeki , accessed 10 January 2023

23 U.S. Department of State, U.S. Support for Connectivity and Cybersecurity in Ukraine, U.S. Department of State Press Releases (10 May 2022) https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/, accessed 9 January 2023

24 Eu4Digital, Improving cyber resilience in the Eastern partnership, EU4 Digital: Cybersecurity East https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/ , accessed 3 January 2023

25 NATO, Ukraine Cyber Defence, NATO Trust Fund (June 2016) - https://www.nato.int/cps/en/natolive/topics_153288.htm, accessed 11 January 2023

26 Microsoft, Defending Ukraine: Early lessons from the cyber war, Microsoft (22 June 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK accessed 12 January 2023

Reference list

Burgess M., 'Hacktivism is Back and Messier Than Ever', Wired (27 November 2022) , https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos, accessed 3 January 2023

Canadian Centre for Cybersecurity, Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine, Canadian Centre for Cybersecurity Centre, (14 July 2022), https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine ,accessed 4 January 2023

Cybersecurity and Infrastructure Security Agency, United States and Ukraine expand cooperation on cybersecurity, Cybersecurity and Infrastructure Security Agency News, (27 July 2022) https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity , accessed 5 January 2023

Duffy. K, A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine, Business Insider (22 April 2022), https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4 , accessed 3 January 2023

European Commission Press Release, 'Cyber Defence: EU boosts action cyber threats', European Commission (10 November 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642 accessed 5 January 2022

European Defence Agency, Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, European Defence Agency News and Events (24 February 2022), https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence , accessed 11 January 2023

EU4Digital, EU supports cybersecurity in Ukraine with over €10 million, EU4Digital News, (21 October 2022) https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/#:~:text=The%20EU%20will%20spend%20more,cybersecurity%20and%20data%20security%20needs. , accessed 10 January 2023

ESET Research, Industroyer 2: Industroyer Reloaded, We Live Security (12 April 2022), https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/, accessed 5 January 2023

Khlemova, I., Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions, State Service of Special Communications and Information Protection of Ukraine, (17 January 2023) https://cip.gov.ua/ua/news/doslidzhennya-zv-yazok-mizh-kiberatakami-konvenciinimi-ta-informaciinimi-atakami-v-ukrayini-vidpovidaye-rosiiskii-koncepciyi-gibridnoyi-viini, accessed 21 January 2023

McEnchroe, T. , Interior Minister: Russia behind cyber-attack on Czech institutions, Radio Prague International (21 April 2022) https://english.radio.cz/interior-minister-russia-behind-cyber-attack-czech-institutions-8748268 , accessed 8 January 2023

Microsoft, Defending Ukraine: Early lessons from the cyber war, Microsoft (22 June 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK accessed 12 January 2023

Microsoft, Special Report: Ukraine, An Overview of Russia's Cyberactivity in Ukraine, Microsoft (27 April 2022) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, accessed 6 January 2023

Microsoft Security Threat Intelligence, New 'Prestige' Ransomware Impacts Organizations in Ukraine and Poland, Microsoft Security [blog post] (14 October 2022), https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/, accessed 10 January 2023

NATO, Madrid Summit Declaration, NATO Official Text (29 June 2022) https://www.nato.int/cps/en/natohq/official_texts_196951.htm, accessed 6 January 2023

NATO, Ukraine Cyber Defence, NATO Trust Fund (June 2016) - https://www.nato.int/cps/en/natolive/topics_153288.htm, accessed 11 January 2023

Security Service of Ukraine, 'SBU cyber specialists upgrade MISP-UA platform: to more effectively protect state authorities from hacker attacks', Security Service of Ukraine (14 June 2021) https://ssu.gov.ua/en/novyny/kiberfakhivtsi-sbu-onovyly-platformu-mispua-shchob-efektyvnishe-zakhyshchaty-orhany-derzhavnoi-vlady-vid-khakerskykh-atak accessed 4 January 2023

State Service of Special Communications and Information Protection of Ukraine, 'Ukraine enhances cooperation with ENISA', State Service of Special Communications and Information Protection of Ukraine News, (7 October 2022) https://cip.gov.ua/en/news/ukrayina-rozvivaye-spivpracyu-z-agentstvom-yes-iz-merezhevoyi-ta-informaciinoyi-bezpeki , accessed 10 January 2023

The Cyberpeace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q3 July to September 2022', Cyberpeace Institute (16 December 2022) https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/, accessed 5 January 2023

Threat Hunter Team Symantec, Ukraine: Disk-wiping Attacks Precede Russian Invasion, Symantec Enterprise Blogs/Threat Intelligence [blog post] (24 February 2022), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia, accessed 8 January 2023

The White House, Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement, White House Briefing Room (25 March 2022) https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/, accessed 10 January 2022

Wolfram. J, Roncone. G, McLellan. T, interview with L. McNamara, 'Threat Trends: Reflections on Russian Cyber Threat Activity During the War in Ukraine ' The Defender's Advantage Podcast, (23 November 2022), Mandiant, https://www.mandiant.com/resources/podcasts/threat-trends-russian-threat-activity-ukraine, accessed 4 January 2023

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 3213 7800
info@globsec.org
www.globsec.org