SIPRI Insights on Peace and Security
No. 2023/09 September 2023

CYBER CROSSOVER AND ITS ESCALATORY RISKS FOR EUROPE

LORA SAALMAN, FEI SU AND LARISA SAVELEVA DOVGAL*

I. Introduction

In recent years, a growing number of cases have highlighted the crossover between cybercrime and cyberwarfare. This has occurred through a merging of tactics commonly associated with cybercrime into operations with distinct cyberwarfare aims. Ongoing tensions in relations of Russia and China with the United States—drawn into high relief with the current war in Ukraine—illustrate a number of these cyber trends. These developments pose a significant challenge for the European Union (EU), which has seen a dramatic increase in the number of cyberattacks since the start of the war.[1] Among these, decoy ransomware and distributed denial of service (DDoS) attacks are increasingly being employed to deliver destructive wipers and remote access trojans (RATs) for cyberwarfare. With such forms of malware widely used by both state and non-state actors, cybercrime and cyberwarfare operations become more and more difficult to disentangle. This growing crossover impacts governance of cyberspace, in which combating cybercrime has historically been one of the few points of international agreement. If cybercrime tactics are used for cyberwarfare aims, managing cyber governance becomes more contentious.

Despite the existing political fissures among the abovementioned actors, there are recent concrete examples of greater coordination within and among the private sector, public sector and international forums. For instance, the EU and the USA have undergone recent synergies, particularly on enhancing the role and responsibilities of the private sector, through the November 2022 Joint Communication on an EU Cyber Defence Policy, the December 2022 update of the EU Network and Information Systems Directive (NIS Directive), and the March 2023 release of the US National Cybersecurity Strategy.[2] This alignment highlights mutual prioritization of public–private sector coordination on cyber resilience, particularly in protection of critical infrastructure. Between governments, an example is the bilateral cooperation between the USA and Russia in January 2022, leading to raids and the arrest of 14 alleged members of the DarkSide and REvil ransomware groups,

SUMMARY

● The crossover between cybercrime and cyberwarfare has intensified in recent years, particularly against the backdrop of the ongoing conflict in Ukraine and mounting tensions between China, Russia and the United States.

This paper delves into specific cyber incidents that employ cybercrime tactics with cyberwarfare objectives, allegedly involving Chinese, Russian or US actors. It examines responses within and among the private sector, the public sector and international forums. Although not directly involved in all of the cases, the European Union (EU) was impacted in a variety of ways, including as a result of spillover effects and intentional targeting. Drawing upon an examination of cyber incidents, this paper highlights how emerging trends in actors, means and responses present escalatory risks for the EU and emphasizes the pressing need to bolster cybersecurity measures.

[1] Thales Group, 'From Ukraine to the whole of Europe: Cyber conflict reaches a turning point', Press release, 29 Mar. 2023.

[2] European Commission, High Representative for Foreign Affairs and Security Policy, 'EU Policy on Cyber Defence', Joint Communication to the European Parliament and the Council, 10 Nov. 2022; and White House, *National Cybersecurity Strategy* (US Government: Washington, DC, Mar. 2023).

* The authors would like to thank the German Federal Foreign Office, which generously provided funding for this project.

including a hacker allegedly involved in the Colonial Pipeline cyberattack.[3] Within international forums, in November 2021 Russia and the USA served as representatives of groups of countries co-sponsoring a draft resolution in the United Nations against the use of information communication technologies (ICTs) for criminal purposes.[4] Further, in November 2022 the US-led Counter Ransomware Initiative issued an action plan on combating ransomware with the participation of 37 states.[5]

To provide greater granularity on the malware and actors driving the above trends, this paper delves into cyber incidents to examine points where cybercrime tactics and cyberwarfare aims merge, with a particular focus on alleged Chinese, Russian and US actors, to identify escalatory risks for Europe.

II. Governance of cybercrime and cyberwarfare

The UN Office on Drugs and Crime (UNODC) defines *cyberwarfare* as ‘cyber acts that compromise and disrupt critical infrastructure systems that amount to an armed attack’, and a *cybercrime* as an ‘act that violates the law, which is perpetrated using ICTs to either target networks, systems, data, websites and/or technology or facilitate a crime’.[6] These definitions are of note, since the UNODC, through its Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs, serves as secretariat for the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Ad Hoc Committee).

While authoritative, the above definitions remain contested, particularly when it comes to cyberwarfare. Accordingly, efforts to counter cybercrime have generally garnered greater support within international governance than efforts against cyberwarfare, particularly through the Budapest Convention on Cybercrime and the follow-on Additional Protocols of the Council of Europe, as well as the efforts of the UNODC’s Ad Hoc Committee.[7] Building on this foundation, since May 2021 UN member states have been negotiating an international treaty on countering cybercrime. If adopted by the UN General Assembly, it would be the first binding UN instrument on a cyber issue.[8] Despite ongoing disagreements over human rights safeguards and data protection, this negotiation carries promise. By contrast, developing norms to regulate cyberwarfare remains much more contentious—par-

[3] Burgess, M., ‘Russia takes down REvil hackers as Ukraine tensions mount’, *Wired*, 14 Jan. 2022; and Dixon, R. and Nakashima, E., ‘Russia arrests 14 alleged members of REvil ransomware gang, including hacker US says conducted Colonial Pipeline attack’, *Washington Post*, 14 Jan. 2022.

[4] United Nations, General Assembly, ‘General Assembly adopts resolution outlining terms for negotiating cybercrime treaty amid concerns over “rushed” vote at expense of further consultations’, Press Release GA/12328, 26 May 2021.

[5] European Commission, ‘International Counter Ransomware Initiative: Strengthening cybersecurity cooperation & actions’, 3 Nov. 2022.

[6] United Nations Office on Drugs and Crime (UNODC), ‘Cyberwarfare’, [n.d.]; and UNODC, ‘Cybercrime in brief’, [n.d.].

[7] Convention on Cybercrime, Budapest, 23 Nov. 2001, *European Treaty Series*, no. 185; and UNODC, ‘Ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes’, [n.d.]. For more information, see Schjolberg, S., ‘A Geneva declaration for cyberspace’, CyberCrime Law, Jan. 2016.

[8] Wilkinson, I., ‘What is the UN cybercrime treaty and why does it matter?’, Chatham House, 2 Aug. 2023.

ticularly among China, Russia and the USA.[9] Such efforts are often driven by Western-led non-official and official initiatives as with, respectively, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the North Atlantic Treaty Organization (NATO) Cyber Defence Pledge, within which Chinese and Russian voices are absent.[10]

Differences in definitions have also translated into varied regulatory approaches at UN level. The issue of information security first appeared on the UN agenda in 1998 with Russia's submission of the first draft resolution, 'Developments in the Field of Information and Telecommunications in the Context of International Security'.[11] The current UN process on cyber governance began in 2004 with governmental groups of experts (GGEs) established by the UN General Assembly. In 2019 the process bifurcated with a US-sponsored GGE—with a limited membership of 25 states—on 'advancing responsible state behaviour in cyberspace in the context of international security' meeting in parallel with a Russian-sponsored open-ended working group (OEWG) on 'developments in the field of information and telecommunications in the context of international security' (OEWG I). Under a second OEWG, on 'security of and in the use of information and communications technology 2021–2025' (OEWG II), Russia and China have articulated concerns about non-governmental organization (NGO) and private sector participation in the process, with Russia blocking the accreditation of 27 NGOs, including the Cybersecurity Tech Accord that represents 150 technology companies, from OEWG II meetings.[12] As private sector involvement increases and blurs the lines between non-combatant and combatant in cyberspace, such differences between governments in recognizing and legislating the role of industry can have a drastic impact on longer-term cyber governance.

This brief discussion highlights the varied stances on cyber governance, stemming from competition in norms and the lack of universally accepted definitions. Despite the lack of unified international approaches, however, cybercrime and cyberwarfare increasingly intersect. Malware frequently identified as part of cybercrime tactics is being used as a decoy for destructive- and exfiltration-related cyberwarfare aims. To elucidate the intersection between cybercrime and cyberwarfare, the following section provides brief case studies involving ransomware, ransomware as a service (RaaS), RATs, DDoS and wiper operations, defined in box 1.

[9] See Giles, K. and Hagestad II, W., 'Divided by a common language: Cyber definitions in Chinese, Russian and English', eds K. Podins, J. Stinissen and M. Maybaum, *2013 5th International Conference on Cyber Conflict: Proceedings* (NATO CCD COE Publications: Tallinn, 2013).

[10] Schmitt, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press: Cambridge, UK, 2017); Schmitt, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press: Cambridge, UK, 2013); and North Atlantic Treaty Organization, 'Cyber Defence Pledge', Press Release no. (2016) 124, 8 July 2016.

[11] Krutskikh, A. V. and Zinovieva, E. S., Eds., 'International Information Security: Russia's Approaches', Moscow State Institute of International Relations, 2021.

[12] UN General Assembly Resolution 75/240, 31 Dec. 2020. On UN GGE and OEWG processes see Pytlak, A., 'Cyberspace and the malicious use of information and communications technology', *SIPRI Yearbook 2022: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2022); UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', [n.d.]; Cybersecurity Tech Accord, 'Industry perspective rejected: Cybersecurity Tech Accord releases joint statement on veto by UN cyber working group', 21 July 2022; and Hurel, L. M., 'The rocky road to cyber norms at the United Nations', Council on Foreign Relations, 6 Sep. 2022.

Box 1. Types of cyber operations and malware described in case studies

Distributed denial of service (DDoS)

A distributed denial of service attack is an attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

Man in the middle (MitM)

Man in the middle attacks involve interception and relay of messages between two parties who believe they are communicating directly with each other.

Ransomware

Ransomware threatens to publish the victim's data or permanently block access to it unless a ransom is paid.

Ransomware as a service (RaaS)

Ransomware as a service is a model in which actors pay or are paid to launch ransomware attacks.

Remote access trojan (RAT)

A remote access trojan is malware designed to allow an attacker to remotely control an infected computer, using a lightweight loader (smaller than 50 kilobytes) to bypass monitoring technologies and to enable the primary malicious code to run on a targeted system.

Wiper

A wiper is malware that erases user data and partition information from attached drives, making the system inoperable and unrecoverable.

Zero-day

'Zero-day' is a broad term encompassing an unknown security vulnerability or software flaw that a threat actor can target with malicious code, named as such since a security team has had '0' days to create a security patch or update to remediate the flaw.

Sources: Baker, K., 'The 12 most common types of malware', Crowdstrike, 28 Feb. 2023; Baker, K., 'Ransomware as a Service (RaaS) explained: how it works and examples', Crowdstrike, 30 Jan. 2023; Crowdflare, 'What is a DDoS attack?', [n.d.]; Checkpoint, 'What is wiper malware?', [n.d.]; and Kaspersky, 'What is a zero-day attack? Definition and explanation', [n.d.].

III. Case studies on cyber incidents

This section presents case studies on cyber incidents allegedly involving Chinese, Russian or US actors. To provide more granularity on each incident, the section examines the responses to the incident within the private sector, the public sector and international forums as applicable. Due to the difficulties of attribution and impacts of cyber incidents across various sectors, the case studies are categorized not by attacker or target, but by the cyber operations and malware described in box 1.

Ransomware and RaaS

Three different but interrelated applications of ransomware cyber incidents are outlined below, the first with a cybercrime aim, the second with cybercrime motives and cyberwarfare effects, and the third with a cyberwarfare aim. In the first case, DoppelPaymer ransomware was used in a blackmail operation that compromised the function of the University Hospital Düsseldorf, contributing to a broader debate in the EU over collateral damage and cybersecurity requirements for critical infrastructure. In the second case, DarkSide ransomware applied an RaaS model for material gain. Since the Colonial Pipeline—a major oil supplier in the USA—was among the victims, this prompted a shutdown that accelerated US legislation on private sector accountability and protection of critical infrastructure against cyberattack. In the third case, Network Battalion 65 employed ransomware to conduct politically motivated hacking activities—also known as hacktivism—against Russia's space agency Roscosmos for cyberwarfare aims.

DoppelPaymer

In September 2020 DoppelPaymer ransomware compromised 30 servers of the University Hospital Düsseldorf using a vulnerability in virtual private network (VPN) software by Citrix.[13] The incident resulted in two weeks of efforts by Germany's Federal Office for Information Security to decrypt the systems, during which the hospital was forced to cancel hundreds of operations and to halt the admission of new patients. Forensic evidence showed the hospital may not have been the primary target and that the cyber operation was executed in error, since a ransom note in one of the compromised servers was addressed to Heinrich Heine University in Düsseldorf.[14] Following the death of one patient, an investigation concluded the patient was so ill that the ransomware attack was not necessarily to blame.[15] Still, this fatality marked a new milestone in collateral damage from cyberattacks.[16] While early reports attributed the cyberattack to Russian sources, the actors were found to be Ukrainian.[17]

Private sector responses. While the Düsseldorf incident occurred in September 2020, DoppelPaymer ransomware was first discovered in June 2019, resulting in a Microsoft Security Response Center warning and guidelines for protecting against the Citrix vulnerability.[18] Initially criticized for its lapse in cyber hygiene, University Hospital Düsseldorf claimed that it had completed the patch—updates that address security vulnerabilities within a program or product—suggesting that the ransomware loader may have been installed prior to the update.[19] Follow-up reports emphasized experts' recommendations that 'organizations in critical sectors' take a more 'proactive' approach based on regular system backups, employee training on avoiding phishing and other scams, and strong passwords.[20]

Public sector responses. In December 2020 the incident was highlighted at the press conference on the EU Cybersecurity Strategy, which proposed review and reform of the NIS Directive to 'provide the basis for more specific rules that will also be expanded to a larger range of strategically important

[13] 'German hospital ransomware attack (2020)', *International Cyber Law in Practice: Interactive Toolkit*, 4 Oct. 2022.

[14] 'The untold story of a cyberattack, a hospital and a dying woman', *Wired*, 11 Nov. 2020.

[15] 'Tödlicher Hackerangriff auf die Uniklinik Düsseldorf?' [Deadly hacker attack on the University Hospital Düsseldorf?], RTL, 17 Sep. 2020.

[16] 'Prosecutors open homicide case after hacker attack on German hospital', Reuters, 18 Sep. 2020.

[17] AFP, 'German experts see Russian link in deadly hospital cyber attack', *The Local*, 22 Sep. 2020.

[18] Microsoft Security Response Center (MSRC), 'Customer guidance for the DopplePaymer ransomware', MSRC Blog, 20 Nov. 2019.

[19] O'Neill, P. H., 'A patient has died after ransomware hackers hit a German hospital', *MIT Technology Review*, 18 Sep. 2020.

[20] CyWare Social, 'A ransomware attack behind death of a patient', CyWare Alerts—Hacker News, 25 Sep. 2020.

sectors'—including healthcare—to enhance the resilience of critical infrastructure.[21]

International forum responses. The incident became part of calls by the International Committee of the Red Cross for a digital emblem and other measures to protect medical facilities, in line with the Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), which prohibits attacks against civilian hospitals and medical transports.[22]

DarkSide

In May 2021 Colonial Pipeline's operators discovered that their network had been compromised by DarkSide ransomware that reportedly had been using an RaaS model for 'financially motivated operations' since at least 2020.[23] To prevent the malware from infecting systems used to control pipeline assets, the 8850-kilometre-long Colonial pipeline—the largest for refined oil products in the USA—was shut down and remained offline for approximately six days. This resulted in gas shortages and rampant gas price increases, with 17 US states declaring a state of emergency. With the hackers threatening to publish the sensitive data that they exfiltrated, Colonial Pipeline paid them approximately $4.4 million in cryptocurrency to get the decryption key. The US Federal Bureau of Investigation (FBI) later managed to retrieve part of the ransom payment.[24]

Private sector responses. Following the incident, Deloitte emphasized the necessity of the private sector engaging in more 'proactive' and 'zero-trust' approaches, even advocating industry to 'go on offense' in hunting for potential threats in their own information technology networks and to consider greater application of machine learning and self-healing systems.[25] In May 2021 the Russian-language user forum called XSS, formerly known as DaMaGeLab, started banning the use of their platforms for purchasing any ransomware tools, due to their 'dangerous and toxic' use.[26]

Public sector responses. In May 2021 US President Joe Biden issued an Executive Order on Improving the Nation's Cybersecurity.[27] By July 2021, the USA had established an Industrial Control Systems Cybersecurity Initiative to

[21] Schinias, M., 'Opening remarks by Vice-President Margaritis Schinas at the press conference on the cybersecurity strategy', Speech, Brussels, 16 Dec. 2020.

[22] International Committee of the Red Cross (ICRC), *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions* (ICRC: Geneva, 2022); and Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, opened for signature 12 Aug. 1949, entered into force 21 Oct. 1950.

[23] Easterly, J. and Fanning, T., 'The attack on Colonial Pipeline: What we've learned & what we've done over the past two years', Cybersecurity & Infrastructure Security Agency (CISA) Blog, 7 May 2023; and Sood, K., Hurley, S. and Arsene, A. L., 'DarkSide goes dark: How CrowdStrike Falcon customers were protected', CrowdStrike, 18 May 2021.

[24] 'The ransomware attack at Colonial Pipeline', Secario Labs, 22 Mar. 2023.

[25] Deloitte, 'Is your critical infrastructure resilient against cyber threats?', [n.d.]. See also Winstead, N., 'Hack-back: Toward a legal framework for cyber self-defense', Center for Security, Innovation and New Technology, American University, 26 June 2020.

[26] Kaspersky ICS CERT, 'DarkChronicles: The consequences of the Colonial Pipeline attack', Report, 21 May 2021.

[27] CISA, 'Executive order on improving the nation's cybersecurity', [n.d.].

buttress the cybersecurity of critical infrastructure.[28] Notably, in January 2022 Russia's Federal Security Service (FSB) responded to US requests to conduct raids and arrested 14 alleged members of the DarkSide and REvil ransomware groups, which included a hacker who allegedly took part in the Colonial Pipeline cyberattack.[29] Signed in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act required US organizations to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and to report ransomware payments within 24 hours.[30] And the US National Cybersecurity Strategy of March 2023 placed a much stronger emphasis on private sector responsibility in preparing for and mitigating cyberattacks on critical infrastructure.[31]

Network Battalion 65

In March 2022 Network Battalion 65 (NB65), a non-state actor reportedly linked to Anonymous, an international hacktivist collective, revealed that they had stolen data from Roscosmos—a government corporation that oversees the Russian space industry—and stated that Russian President Vladimir Putin 'no longer has control over spy satellites'.[32] NB65 shared a tweet containing information purportedly taken from a server of the Russian space agency's WS02 vehicle monitoring system.[33] Some cyber expert reports claim that the source code for the attack was made up of 66 per cent 'of the same code as that of Conti'—alleged Russian ransomware—suggesting that NB65 likely purchased Conti ransomware from a supplier offering RaaS services.[34] While NB65 did seem to have exfiltrated documents and administration materials, currently available evidence does not suggest that they gained control over Roscosmos operational systems and satellites.[35]

Public sector responses. The then director-general of Roscosmos, Dmitry Rogozin, tweeted a March 2022 response to NB65 claims regarding the space agency, stating that 'the information published by these fraudsters and pretty swindlers is false. All our space control centers operate as usual'.[36] While denying the cyberattacks, Rogozin later that month stated that 'Offlining the satellites of any country is actually a casus belli, a cause for war'.[37] In the same month, Rogozin declared in another interview that Russia needed an 'independent, sovereign space Internet network', which could be achieved

[28] White House, 'National security memorandum on improving cybersecurity for critical infrastructure control systems', Briefing Room Statement, 28 July 2021.

[29] Burgess (note 3); and Dixon, and Nakashima (note 3).

[30] CISA, 'Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)', Fact sheet, Jan. 2023.

[31] White House, *National Cybersecurity Strategy* (note 2).

[32] Allen, I., 'Russia targeted by unprecedented wave of cyber-attacks, experts say', *IntelNews*, 3 May 2022.

[33] AnonymousTV, Twitter, 1 Mar. 2022; and Johnson, B., 'Anonymous vs. Russia: Hackers say space agency breached, more than 1,500 websites hit', *Homeland Security Today*, 1 Mar. 2022.

[34] Goud, N., 'Anonymous used Conti ransomware to down Russian satellites', Cybersecurity Insiders, [n.d.].

[35] Bender, B., 'Russia's space chief says hacking satellites "a cause for war"', *Politico*, 2 Mar. 2022.

[36] Smith, A., 'Anonymous hackers claim attack on Russia's space agency but Roscosmos chief calls them 'fraudsters and swindlers', *The Independent*, 2 Mar. 2022.

[37] 'Russia space agency head says satellite hacking would justify war—report', Reuters, 2 Mar. 2022.

by launching new satellite constellations.[38] On 1 May 2022 Russia issued Presidential Decree No. 250 mandating additional requirements regarding the origins of software and hardware used for cyber defence in critical information infrastructure (CII).[39] The decree required both public and private sector CII organizations to establish information security departments responsible for detection, prevention and recovery from cyberattacks.

Ransomware and RATs

In the two cases outlined below, the combination of ransomware and RATs indicate entanglement of cybercrime tactics and cyberwarfare aims. In the first case, Bronze Starlight's use of ransomware departed from the usual aim of encrypting data for material gain. Instead, it used allegedly Chinese-origin ransomware as a decoy to mask the targeted planting of a RAT for exfiltration of data of multiple industries, including aerospace and defence. In the second case, China's Northwestern Polytechnical University (NPU), which has purported ties to China's People's Liberation Army (PLA), was allegedly targeted with ransomware and RATs as well as a host of other tools. While intellectual property theft was part of the likely aims, the nature of the data stolen suggests potential military applications.

Bronze Starlight

Active since 2021, Bronze Starlight has been observed using 'ransomware and double extortion as a cover to steal data from organizations of interest to China and destroy evidence of its activity'.[40] Among the more than 21 targeted companies were Japanese and Lithuanian electronic component designers and manufacturers, as well as the aerospace and defence division of an Indian conglomerate.[41] Bronze Starlight used the ransomware as a decoy to deploy a HUI loader along with a relatively rare version of PlugX—a RAT allegedly linked to China-backed threat groups—and periodically updated its HUI loader with detection evasion techniques.[42] This approach of using targeted campaigns with evolving tactics, according to SecureWorks, is the hallmark of state-sponsored activities.[43] Forensic reports are conflicting, due to the number of names associated with this advanced persistent threat (APT) group; nevertheless a number of reports link Bronze Starlight to

[38] 'Рогозин пообещал создать для России «неубиваемый» интернет' [Rogozin promised to create an 'indestructible' Internet for Russia], *Izvestia*, 10 Mar. 2022.

[39] Legislative Acts of the Russian Federation, 'Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"' [Decree of the President of the Russian Federation of 01.05.2022 No. 250 'On additional measures to ensure information security of the Russian Federation'], 1 May 2022.

[40] Vijayan, J., 'US accuses China of using criminal hackers in cyber espionage operations', *DarkReading*, 19 July 2021; and Vijayan, J., 'Chinese APT group likely using ransomware attacks as cover for IP theft', *DarkReading*, 23 June 2022.

[41] Nichols, S., 'Chinese HUI loader malware ups the ante on espionage attacks', TechTarget, 23 June 2022; and SecureWorks, Counter Threat Unit Research Team, 'Bronze Starlight ransomware operations use HUI loader', Threat Analysis, 23 June 2022.

[42] Lakshmanan, R., 'State-backed hackers using ransomware as a decoy for cyber espionage attacks', *Hacker News*, 24 June 2022; Vijayan, 'US accuses China of using criminal hackers in cyber espionage operations' (note 40); and Vijayan, 'Chinese APT group likely using ransomware attacks as cover for IP theft' (note 40).

[43] SecureWorks, Counter Threat Unit Research Team, 'Bronze Starlight ransomware operations use HUI loader' (note 41).

APT10, which allegedly has ties to China's Ministry of State Security (MSS).[44] They also indicate that Bronze Starlight may be connected with Cicada, Cloud Hopper, Red Apollo, CNVX, Stone Panda, MenuPass, POTASSIUM, MenuPass Group and Emperor Dragonfly. Its HUI loader is also allegedly the same as that used by Bronze Riverside, which is also known as APT41.

Private sector responses. Forensic reports focus on Bronze Starlight's use of known vulnerabilities. Supported by findings from CISA advisories, SecureWorks has emphasized that cyber operations from alleged Chinese actors often exploit vulnerabilities that already have a patch available, instead of zero-day vulnerabilities that often receive the most attention.[45] Their report highlights the importance of companies establishing multi-layered cybersecurity practices and both consistent and persistent patching of vulnerabilities, such that hackers are forced to break through multiple layers of security—physical, administrative and technical—making it more difficult for them to gain and sustain access.

Public sector responses. Many of these pre-date reports on Bronze Starlight, targeting broader APT campaigns with which it may be linked. As one example, in 2018 the US Department of Justice (DOJ) charged two Chinese members of APT10 associated with the MSS's Tianjin Bureau with engaging in 'global computer intrusions'.[46] The DOJ also reported details of cyber operations that engaged in data exfiltration from managed service providers and over 45 technology companies, stealing 'hundreds of gigabytes of sensitive data' and targeting 'the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology and maritime technology'.[47]

SecondDate, Drinking Tea

In June 2022 China's National Computer Virus Emergency Response Centre (CN-CVERC), in cooperation with the Chinese cybersecurity company Qihoo 360 Security Technology Inc. (Qihoo 360), detected cyberattacks on China's NPU, allegedly tracing them to the US National Security Agency (NSA) Office of Tailored Access Operations.[48] The reports suggest that the cyberattack targeted a zero-day vulnerability at the university, using servers in 17 countries including Japan, South Korea, Sweden, Poland, Ukraine and Colombia to conduct the attack. *Global Times* reporting draws from unnamed sources to describe such alleged NSA tools as SecondDate for 'man in the

[44] CyWare, 'APT10: A Chinese threat on a global espionage mission', Blog, 8 Aug. 2022; Balaji, N., 'Bronze Starlight—Chinese APT using short-lived ransomware families for cyberespionage activities', Cyber Security News, 27 June 2022; and Telychko, V., 'Cheerscrypt ransomware detection: China-backed hackers, Emperor Dragonfly aka Bronze Starlight, are behind ongoing cyber attacks', SOC Prime, 5 Oct. 2022.

[45] CISA, 'Top CVEs actively exploited by People's Republic of China state-sponsored cyber actors', Alert no. AA22-279A, 6 Oct. 2022.

[46] US Department of Justice, Office of Public Affairs, 'Two Chinese hackers associated with the Ministry of State Security charged with global computer intrusion campaigns targeting intellectual property and confidential business information', Press release, 20 Dec. 2018.

[47] US Department of Justice, Office of Public Affairs (note 46).

[48] Zhadan, A., 'China claims 13 NSA operators hacked into university', CyberNews, 28 Sep. 2022.

middle' (MitM) attacks and Drinking Tea as a RAT.[49] By contrast, forensic reports from Qihoo 360 provide much greater detail on the cyberattack vectors to allege that the 41 'network attack' tools also included the NSA's Ebbshave, Ebbisland, FoxAcid, NOPEN Trojan, DanderSpritz, Stoicsurgeon and Toast, among others.[50]

Private sector responses. Qihoo 360 and the CN-CVERC reportedly identified at least 50 APTs targeting China, including those allegedly launched by the NSA and the Central Intelligence Agency (CIA).[51] Its initial report contained a general history of alleged NSA and CIA cyber operations and a list of connected malware, with a follow-up report containing specifics on malware types, dates and times of incursion, as well as partial internet protocol (IP) addresses employed in cyber operations against NPU.[52] This marked a milestone in China's approach towards attribution, in that Qihoo 360 is a private Chinese company that publicly released detailed forensic reports.[53] Further, Qi An Xin Technology also attributed these cyberattacks to the NSA, providing analysis on other alleged US cyber operations.[54]

Public sector responses. A Chinese foreign ministry spokesperson stated that the actions by the US agencies identified in the reports 'seriously endanger China's national security', and condemned 'the NSA's cyber attacks and data theft against China', alleging the involvement of 13 US personnel, 'more than 60 contracts and more than 170 digital documents with US telecom operators to build an environment for cyber attacks', and over 1000 cyberattacks against NPU to steal 'core technical data'.[55] Coinciding with the 2022 China Cybersecurity Week, the statement called for increased efforts to 'enhance the cybersecurity awareness and protection capacity of the whole society'.[56] One Chinese expert has suggested that this represents the first time the Chinese Government has backed up public attribution for a cyberattack with forensic detail from private industry.[57]

[49] Cao, S. Q., 'Exclusive: "Concealed, adaptable" weapon of NSA's cyberattack on leading Chinese aviation university exposed', *Global Times*, 13 Sep. 2022.

[50] Qihoo 360, '关于西北工业大学发现美国NSA网络攻击调查报告（之一）' [Investigative report on Northwestern Polytechnical University's discovery of the US NSA's cyberattack (Part 1)], 5 Sep. 2022; and Qihoo 360, '西北工业大学遭受美国NSA网络攻击调查报告（之二）' [Investigative report on Northwestern Polytechnical University's suffering from US NSA's cyberattack (Part 2)], 27 Sep. 2022.

[51] Guancha, '360周鸿祎讲述：如何抓住网络攻击西工大的幕后黑手？' [Qihoo 360 Zhou Hongwei: How to catch the mastermind behind the network attack on Northwestern Polytechnical University?], 15 Sep. 2022.

[52] Qihoo 360, Investigative report part 1 and 2 (note 50).

[53] 'Chinese tech company Qihoo 360 latest to be taken private', Reuters, 18 Dec. 2015; and Qihoo 360, Investigative report parts 1 and 2 (note 50).

[54] '分析报告发布 透露西北工大遭美网袭事件新细节' [Analysis report reveals new details of the Northwestern Polytechnical University cyberattack by the US], Sina, 13 Sep. 2022; and Antiy Labs, '安天分析美方网空攻击活动成果' [Antiy's analysis of the results of US cyberspace attack activities], 13 Sep. 2022.

[55] Mao Ning, Chinese Foreign Ministry Spokesperson, Statement at Press Conference, Vanuatu, 5 Sep. 2022.

[56] Mao Ning (note 55).

[57] View of cybersecurity expert from China, expressed at the workshop 'Cyber Incidents and Threat Perceptions: Views from China, Russia, Europe and the United States', SIPRI, Stockholm, 13–14 June 2023.

Ransomware and wipers

In the two cases below ransomware was deployed as a decoy for delivering wipers with cyberwarfare aims. In the first case, WhisperGate wiper attacks masqueraded as ransomware threatening to encrypt the master boot record (MBR) for ransom, but aimed to render operating systems in Ukraine inoperable the month prior to the 2022 Russian invasion. In the second case, the FoxBlade wiper—with alleged links to Russian intelligence—was paired with decoy ransomware deployed early in the invasion, destroying systems and data across several sectors in Ukraine, Latvia and Lithuania. Both attacks demonstrate how ransomware, originally designed to temporarily deny access to systems and data through encryption, was used to disguise destructive wipers to facilitate military operations.

WhisperGate

In January 2022 Microsoft identified a destructive malware operation, known as WhisperGate, aimed at multiple organizations in Ukraine, including those belonging to the Ukrainian Ministry of Foreign Affairs, Ministry of Defence, State Emergency Service, Cabinet and Ministry of Energy.[58] These wiper attacks disguised as ransomware, coupled with phishing scams, exploits and supply chain attacks, claimed to encrypt a victim computer's MBR, which is the first sector on a hard drive containing essential code to start the operating system, unless a ransom was paid. However, multiple forensic reports showed that the actual aim was to destroy the MBR, since the malicious bootloader—a segment of codes in the microcontroller which runs before application program—used in the attack corrupted the MBR and lacked a decryption mechanism, rendering data retrieval impossible.[59]

Private sector responses. Companies like Microsoft played a key role in identifying WhisperGate cyber operations and compromised targets within Ukraine, as a result of both their contractual obligations towards Ukrainian customers and the companies' own initiatives to assist Ukraine in rebuffing the cyberattacks.[60] While SecureWorks noted that it was unlikely that organizations outside of Ukraine would be directly targeted, warnings emerged of 'exposure to collateral damage from attacks launched in Ukraine that could spread to global operations' including business partners and service providers in Ukraine.[61] As a result, the firm advocated for robust network segmentation, patching internet-facing systems against known vulnerabilities, implementing and maintaining antivirus solutions, and monitoring endpoint detection.

[58] Microsoft, Digital Security Unit, 'Destructive malware targeting Ukrainian organizations', Microsoft Security Blog, 15 Jan. 2022.

[59] Mandiant Threat Intelligence, 'Evacuation and humanitarian documents used to spear phish Ukrainian entities', Mandiant Blog, 20 July 2022; Microsoft, Digital Security Unit, 'An overview of Russia's cyberattack activity in Ukraine', Special report: Ukraine, 27 Apr. 2022; and CrowdStrike, 'Technical analysis of the WhisperGate malicious bootloader', Crowdstrike Blog, 19 Jan. 2022.

[60] Views of a cybersecurity expert from Europe expressed at the 'Cyber Incidents and Threat Perceptions' workshop (note 57).

[61] SecureWorks, Counter Threat Unit Research Team, 'Disruptive attacks in Ukraine likely linked to escalating tensions', SecureWorks Blog, 21 Jan. 2022.

Public sector responses. In February 2022, in the wake of the WhisperGate cyberattacks, Mykhailo Fedorov, Ukrainian vice-prime minister and minister of digital transformation, called for the formation of an Information Technology Army of Ukraine (IT Army), an international crowdsourced community of hackers that allegedly came to include the Anonymous hacker group.[62] Officials from the Ukrainian Ministry of Defence also reportedly approached Yegor Aushev, a Ukrainian businessman and cybersecurity expert, to help organize the IT Army via a Telegram channel listing new Russian targets for volunteers to attack.[63] In the USA, the CISA advised US entities working with Ukrainian organizations to 'take extra care to monitor, inspect, and isolate traffic from those organizations; [and] closely review access controls for that traffic'.[64] And, in January 2022 the Council of the EU released a declaration strongly condemning attacks against Ukrainian government websites, while confirming the EU's intent to 'provide additional, direct, technical assistance to Ukraine to remediate this attack and to support Ukraine against any destabilizing actions, including by further building up its resilience against hybrid and cyber threats'.[65]

FoxBlade

In February 2022, several hours before the launch of the Russian invasion of Ukraine, offensive and destructive cyberattacks were directed against Ukraine's civilian digital infrastructure. Notable among these was the FoxBlade wiper, also known as HermeticWiper, which allegedly has links to Russian military intelligence.[66] Coupled with decoy ransomware, FoxBlade destroyed systems and information across more than 12 organizations in government, ICT, energy, agricultural and financial sectors in Ukraine, and also appeared in Latvia and Lithuania.[67] The Iridium group—allegedly connected to the Sandworm hacking unit (also known as Unit 74455) of Russia's military intelligence agency, the Main Directorate of the General Staff of the Armed Forces—is thought to be linked to the deployment in Ukraine of not only FoxBlade, but also such wipers as CaddyWiper and Industroyer2.[68]

[62] Brewster, T., '"If Kyiv falls, we keep hacking Putin": On the cyber front line in Ukraine', *Forbes*, 25 Feb. 2022; Miller, M., 'Ukraine's largest telecom stands against Russian cyberattacks', *Politico*, 7 Sep. 2022; and Soesanto, S., *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, Cyberdefense Report (Center for Security Studies and ETH Zürich: Zürich, June 2022).

[63] Reuters, 'Ukrainian cyber resistance group targets Russian power grid, railways', *Gadgets360*, 2 Mar. 2022.

[64] CISA, 'Implement cybersecurity measures now to protect against potential critical threats', CISA Insight, 18 Jan. 2022.

[65] Council of the European Union, 'Ukraine: Declaration by the High Representative on behalf of the European Union on the cyberattack against Ukraine', Press release, 14 Jan. 2022.

[66] Constantinescu, V., 'New FoxBlade malware hit Ukraine hours before invasion, Microsoft says', BitDefender Blog, 1 Mar. 2022; 'DoS:Win32/FoxBlade.A!dha', Microsoft Security Intelligence, 23 Feb. 2022; and Guerrero-Saade, J. A., 'HermeticWiper—New destructive malware used in cyber attacks on Ukraine', Sentinel Labs, 23 Feb. 2022.

[67] Microsoft, Digital Security Unit, 'An overview of Russia's cyberattack activity in Ukraine' (note 59); and Uchill, J., 'Ransomware may have been a decoy to launch new wiper malware seen in Ukraine cyberattacks', SC Media, 24 Feb. 2022.

[68] Microsoft, Digital Security Unit; 'An overview of Russia's cyberattack activity in Ukraine' (note 59); Holt, R., 'Sandworm: A tale of disruption told anew', WeLiveSecurity by ESET, 21 Mar. 2022; and CISA, 'New Sandworm malware Cyclops Blink replaces VPNFilter', Alert no. AA22-054A, 23 Feb. 2022.

Private sector responses. Microsoft issued a statement in February 2022 explaining the actions it was taking in four areas: securing Ukraine from cyberattacks; defending against state-sponsored disinformation campaigns; providing support for humanitarian assistance; and protecting Microsoft employees in Ukraine, Russia and 'the broader region'.[69] Following its analysis of offensive and destructive cyberactivity in Ukraine, Microsoft also issued guidance on best practices.[70] While noting that Microsoft is 'a company and not a government or a country', the statement highlighted that its response involved close consultation with the Ukrainian government, the EU, European states, the US government, NATO and the UN. This included taking control of internet domains and creating 'sinkholes' that capture malicious traffic.

Public sector responses. In February 2022 the US deputy national security adviser for cyber and emerging technologies, Anne Neuberger, reportedly asked whether Microsoft would consider sharing details of the FoxBlade code with Estonia, Latvia, Lithuania, Poland and other European states, to address US concerns that the malware would spread beyond Ukraine's borders and cripple NATO or West and Central European banks.[71] General Paul Nakasone of the US Cyber Command stated in a June 2022 interview that the USA had conducted 'hunt forward' operations 'across the full spectrum; offensive, defensive, [and] information operations', to deter Russian cyberattacks against Ukraine.[72] These consisted of US Cyber Command's Cyber National Mission Force (CNMF) operators 'sit[ting] side-by-side with partners and hunt[ing] for vulnerabilities, malware, and adversary presence on the host nation's networks'.[73] In March 2022 the Estonian e-Governance Academy began implementing a €10 million EU project to strengthen cybersecurity and to keep public services available in Ukraine.[74] In December 2022 the EU also unveiled a cyber laboratory in Kyiv to develop Ukraine's cyber defence capacities.[75] In May 2023 Ukraine formally joined NATO's Cooperative Cyber Defence Centre of Excellence.[76] And in April 2023 the US CNMF dispatched around 40 more specialists to Ukraine to help combat Russia's alleged cyber operations.[77]

International forum responses. While not specifically targeted at 'decoy ransomware', the Counter Ransomware Initiative summit in October and November 2022 highlighted the type of public–private sector cooperation evident in the coordination between Microsoft and the US government on

[69] Smith, B., 'Digital technology and the war in Ukraine', Microsoft on the Issues Blog, 28 Feb. 2022.

[70] Microsoft Security Response Center (MSRC), 'Cyber threat activity in Ukraine: Analysis and resources', MSRC Blog, 28 Feb. 2022.

[71] Sanger, D. E, Barnes, J. E. and Conger, K., 'As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war', *New York Times*, 28 Feb. 2022.

[72] Martin, A., 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', Sky News, 1 June 2022.

[73] US Cyber Command Public Affairs, 'Cyber 101: Hunt forward operations', News, 15 Nov. 2022.

[74] EU4Digital, 'EU supports cybersecurity in Ukraine with over €10 million', 21 Oct. 2022.

[75] European External Action Service, 'Ukraine: EU sets up a cyber lab for the Ukrainian armed forces', Press release, 2 Dec. 2022.

[76] AFP, 'Ukraine joins NATO cyber-defense center', *Defense Post*, 17 May 2023.

[77] 'US deploys more cyber forces abroad to help fight hackers', Channel News Asia, 25 Apr. 2023.

the FoxBlade wiper, which was deployed using decoy ransomware.[78] The participation of 37 countries, the timing of the summit and its resulting action plan have the potential to strengthen measures against such decoy ransomware operations, through (*a*) holding ransomware actors accountable for their crimes and not providing them safe haven; (*b*) disrupting and bringing to justice ransomware actors and their enablers; and (*c*) collaborating in 'disrupting ransomware by sharing information, where appropriate and in line with applicable laws and regulations, about the misuse of infrastructure to launch ransomware attacks to ensure national cyber infrastructure is not being used in ransomware attacks'.[79]

DDoS, ransomware and wipers

In the following two cases, DDoS and ransomware attacks were used as decoys for destructive cyberwarfare operations as part of the Ukraine conflict, resulting in collateral damage. In the first case, the broadband network operated on behalf of US satellite communications company Viasat—which provided services to Ukraine agencies, among other clients—became the target of a DDoS cyberattack used to deliver AcidRain wiper malware that eventually affected European industries outside Ukraine. In the second case, Killnet also undertook DDoS attacks, followed by ransomware operations, against government, industry, banking, hospital and airport infrastructure in a number of countries that support Ukraine. Together these cyberattacks represent the culmination of cybercrime tactics—namely DDoS, ransomware and wipers—utilized for cyberwarfare aims.

AcidRain

Coinciding with the invasion of Ukraine in February 2022, a cyberattack targeted the KA-SAT satellite broadband network that is operated on the US company Viasat's behalf by Skylogic, a subsidiary of French satellite operator Eutelsat.[80] The DDoS attack was detected when high volumes of focused, malicious traffic emanated from several modems and other customer equipment physically located within Ukraine and serviced by one of the KA-SAT consumer-oriented network partitions.[81] While likely targeted at the Ukrainian military's satellite communications, the cyberattack impacted 'several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe'.[82] It disrupted emergency services in France and interrupted remote monitoring and control of 5800 wind turbines in Germany.[83] Viasat initially found that the malware 'over-

[78] European Commission, 'International Counter Ransomware Initiative: Strengthening cybersecurity cooperation & actions' (note 5).

[79] European Commission, 'International Counter Ransomware Initiative: Strengthening cybersecurity cooperation & actions' (note 5).

[80] Viasat, 'KA-SAT network cyber attack overview', 30 Mar. 2022.

[81] Viasat (note 80).

[82] Viasat (note 80).

[83] French National Assembly, National Defence and Armed Forces Committee, 'Compte rendu: Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale' [Report: Closed doors hearing of Mr Stéphane Bouillon, secretary-general for defence and national security], Report no. 5, Extraordinary session of 2021–22, 13 July 2022; and Enercon, 'Over 95 per cent of WECs back online following disruption to satellite communication', 19 Apr. 2022.

wrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable'.[84] However, on further investigation, Sentinel Labs maintained that the cyberattack used the KA-SAT management mechanism in a supply chain attack to push the destructive AcidRain wiper, which is designed to render the modems inoperable. These findings also note that the attacks may have had Russian sources.[85]

Private sector responses. Given that the AcidRain wiper used a known vulnerability, cybersecurity companies have emphasized the importance of minimizing unpatched vulnerabilities.[86] One report highlighted cyber vulnerabilities within the larger space industry as a whole, which is privately and publicly owned, complicating the industry's efforts to improve its overall cybersecurity posture.[87] In an instance of private–public sector collaboration, Viasat is reportedly working with the US government's Air Force Research Laboratory under a seven-year $50.8 million contract to develop concepts for 'hybrid networks' of commercial and government-owned satellites.[88]

Public sector responses. While Russia did not claim responsibility for the cyberattack, several states—including member states of the EU, the United Kingdom and the USA—attributed the attack to Russia.[89] In March 2022, the CISA issued a report and warning for US satellite operators that contained risk mitigation measures including log monitoring, encryption and secure methods of authentication. It also requested that 'all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity'.[90] In May 2022 the Council of the EU released a new declaration condemning the cyberattack and noting the dangers of the indiscriminate communication outages and disruptions affecting both public and private sectors in Ukraine and EU member states.[91] The EU stressed that it was considering 'further steps to prevent, discourage, deter and respond to such malicious behaviour in cyberspace'.[92]

International forum responses. The Viasat cyberattack illustrates hurdles to regulation in that space systems often serve both civilian and military

[84] Viasat (note 80).

[85] Guerrero-Saade, J. A. and van Amerongen, M., 'AcidRain—a modem wiper rains down on Europe', Sentinel Labs, 31 May 2022.

[86] Poireault, K., 'Five takeaways from the Russian cyber-attack on Viasat's satellites', *InfoSecurity Magazine*, 9 May 2023.

[87] Gallant, B., 'The growth of the space economy and new cyber vulnerabilities', CIGI Online, 29 Jan. 2023.

[88] Erwin, S., 'Cyber warfare gets real for satellite operators', *SpaceNews*, 20 Mar. 2022.

[89] Council of the European Union, 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', Press release, 10 May 2022; British Foreign, Commonwealth and Development Office, 'Russia behind cyberattack with Europe-wide impact an hour before Ukraine invasion', Press release, 10 May 2022; and Blinken, A. J., US Secretary of State, 'Attribution of Russia's malicious cyber activity against Ukraine', Press statement, US Department of State, 10 May 2022.

[90] CISA, 'Strengthening cybersecurity of SATCOM network providers and customers', Alert no. AA22-076A, 10 May 2022.

[91] Council of the European Union, 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union' (note 89).

[92] Council of the European Union, 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union' (note 89).

functions and have users in multiple states that may not be involved in a conflict. This dual-use nature of space systems, particularly satellite services, becomes complicated under international humanitarian law (IHL), which prohibits targeting of civilian objects but not those of dual-use objects if they qualify as a military objective by nature, location, purpose or use.[93] This argument is reflected in the statement by the Russian deputy head of delegation at the September 2022 second session of the OEWG on reducing space threats through norms, rules and principles of responsible behaviours, who claimed: 'Quasi-civilian infrastructure may become a legitimate target for retaliation'.[94]

KillNet

In February 2022 the KillNet hacker group began performing DDoS attacks on government, industry, banking, hospital and airport infrastructure in countries that support Ukraine, including Italy, Germany, the Netherlands, Poland and the USA. In June 2022, following the Kaliningrad transit crisis—when Lithuania decided to block certain goods on the EU sanctions list from transiting its territory to Russia—the group conducted a DDoS attack on Lithuanian public and private websites.[95] Days after the destruction of the Kerch bridge in October 2022, KillNet also launched a series of DDoS attacks on US airports.[96] In November 2022 KillNet claimed responsibility for taking down the website of the European Parliament in a DDoS attack that came just hours after the legislative body declared Russia a terrorist state.[97] And in January 2023 another series of DDoS attacks against German government websites, banks and airports came shortly after its decision to supply tanks to Ukraine.[98] While the CISA claimed that these incidents only temporarily reduced the availability of certain websites, their widespread nature and impact on critical infrastructure indicate the inherent dangers of such activities.[99] Further, while Killnet initially focused on DDoS attacks, by the end of October 2022 PCrisk had discovered the first sample of KillNet ransomware, which Acronis reported was in fact a wiper designed to overwrite files with random data, making them unrecoverable. Acronis concluded that the absence of payment information in the malware suggested that KillNet did not seek financial benefits, but instead data destruction.[100]

[93] Protocol I Additional to the 1949 Geneva Conventions and Relating to the Protection of Victims of International Armed Conflicts, opened for signature 12 Dec. 1977, entered into force 7 Dec. 1978, Articles 48 and 52.

[94] Vorontsov, K. V., Statement at the second session of the open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, Geneva, 12 Sep. 2022.

[95] Euronews with AP and AFP, 'Lithuania hit by cyberattacks amid Kaliningrad sanctions feud with Russia', Euronews, 28 June 2022.

[96] Vijayjan, J., 'US airports in cyberattack crosshairs for pro-Russian group Killnet', *DarkReading*, 10 Oct. 2022.

[97] Asokan, A., 'Russian KillNet shuts down EU Parliament website with DDoS', Gov Info Security, 23 Nov. 2022.

[98] Gyongyoși, L., 'Killnet Russian hacking group launches DDoS attacks on German websites', Heimdal, 26 Jan. 2023.

[99] Greig, J., 'CISA says Killnet DDoS attacks on US hospitals had little effect', *The Record*, 7 Feb. 2023.

[100] Acronis Security Team, 'Killnet ransomware—a wiper from the Chaos family', Acronis Malware Analysis, 25 Nov. 2022.

Private sector responses. A number of cybersecurity providers responded to the KillNet cyberattacks with advice. For example, Acronis emphasized that a multi-layered approach to cybersecurity to address 'never-before-seen' ransomware and wiper threats is essential.[101] Avertium advocated the application of monitoring software as well as various security information and event management systems to detect the attacks as early as possible.[102] Other firms highlighted the need for 'proactive defence' against DDoS within industry through active intelligence-gathering on potential cyber threats.[103]

Public sector responses. Facing similar threats across a range of DDoS cyberattacks, in October 2022 the CISA updated its DDoS capacity enhancement guides for organizations and federal agencies, offering additional steps that should be taken before, during and after a potential DDoS attack.[104] In November 2022, in direct response to the KillNet attacks, the president of the European Parliament, Roberta Metsola, tweeted that her organization had undergone a 'sophisticated' cyberattack and provided both attribution and motivation for the cyberattack through a political statement: 'A pro-Kremlin group has claimed responsibility. Our IT experts are pushing back against it & protecting our systems. This, after we proclaimed Russia as a state-sponsor of terrorism'.[105]

IV. Escalatory risks for Europe

As the EU continues to develop its regulatory responses in the cyber domain, it should factor in the escalatory risks of cyber incidents on the cybersecurity landscape. While the EU was not the direct target of all the cyber incidents outlined above, it was impacted in a variety of ways. This section analyses these incidents for their escalatory risks in terms of actors, means and responses.

Actors

Targeting of the EU

The ongoing war in Ukraine has resulted in increased malicious cyber activities against the EU, including cyberattacks against its member states.[106] In particular, the KillNet DDoS, ransomware and wiper attacks against EU member states and the European Parliament stemmed from geopolitical tensions arising from their support of Ukraine. According to Thales Group, cyberattacks targeting EU countries increased dramatically, from 9.8 per

[101] Acronis Security Team (note 100).

[102] Avertium, 'An in-depth look at Russian threat actor, Killnet', 18 Oct. 2022.

[103] Rohner, N., 'Russian hacktivist group KillNet hits US hospitals with DDoS attacks', BlackBerry Blog, 14 Feb. 2023.

[104] CISA, FBI and Multi-State Information Sharing & Analysis Centre, 'Understanding and responding to distributed denial-of-service attacks', 28 Oct. 2022.

[105] Kelly, R., 'Killnet group claims responsibility for European Parliament cyber attack', DIGIT News, 24 Nov. 2022.

[106] Council of the European Union, 'Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine', Press release, 19 July 2022; and Smith, B., 'Defending Ukraine: Early lessons from the cyber war', Microsoft On the Issues Blog, 22 June 2022.

cent to 46.5 per cent of global attacks, in 'the last six months' of 2022.[107] While the bulk of these cyberattacks were DDoS, a Thales Group report also cites cases of data exfiltration, espionage, destructive wipers, defacement, influence operations, spear-phishing and phishing, and ransomware being deployed across an increasing diversity of sectors. Those impacted included banking and finance, civil society, defence, education and research, energy, healthcare, industry, aviation and space, telecommunications, transportation, media, public and local administration, among other sectors.[108] Given the scope of these cyberattacks and the prevalence of decoy ransomware and DDoS delivering destructive wipers and RATs among the cases above, the risk of these various tactics merging into longer-term security threats for the EU is substantial. Beyond the context of the Ukraine war and deteriorating relations with Russia, EU engagement in the Asia-Pacific may also elicit such cyberattacks in future. As one example, the 2022 annual threat landscape report of the EU Agency for Cybersecurity (ENISA) identified the development of state-sponsored threat actors targeting 'Member States of the EU that had established closer ties with Taiwan' with cyber operations.[109] As argued by one European expert, this trend is only likely to grow with intensifying geopolitical tensions.[110]

Non-state actors

Official calls in Ukraine for the formation of an IT Army, as a nexus of state and non-state actors, complicates already contentious UN norm-building efforts, particularly when it comes to cyberattacks on civilian critical infrastructure. According to the Ukrainian Ministry of Digital Transformation, by late February 2022 the IT Army had conducted offensive cyber operations against Russian and Belarusian state services websites; financial targets including the Moscow Stock Exchange, Sberbank, the BestChange cryptocurrency exchange and the Belarusian National Bank; the websites of the FSB, Roskomnadzor (the Russian media regulation agency), the Russian president, the Russian government and the Russian parliament; and media organizations including TASS, Kommersant and Fontanka.[111] The targets cited for cyberattack by the IT Army have also included railways and the power grid.[112] When it comes to cyberattacks on civilian critical infrastructure, some of these operations arguably violate the law of armed conflict and 'could amount to unlawful attacks against civilian objects if they are reasonably expected to cause injury or damage, or they might otherwise breach the duty to take constant care to protect civilians

[107] Thales Group (note 1).

[108] Thales Cyber Threat Intelligence Team, '2022–2023: A year of cyber conflict in Ukraine', Thales Group Summary Report, Feb. 2023.

[109] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022 (July 2021 to July 2022)* (ENISA: Athens, Nov. 2022).

[110] 'Hacktivism is back and messier than ever', *Wired*, 27 Dec. 2022; and Views expressed by a cybersecurity expert from Europe at the 'Cyber Incidents and Threat Perceptions' workshop (note 57).

[111] Ukrainian Ministry of Digital Transformation, 'IT army blocks Russian sites in a few minutes—the main victories of Ukraine on the cyber front', 28 Feb. 2022.

[112] Schectman, J., Bing, C. and Pearson, J., 'Ukrainian cyber resistance group targets Russian power grid, railways', Reuters, 1 Mar. 2022; and Council on Foreign Relations, 'Ukrainian IT Army', Cyber Operations Tracker, [n.d.].

and civilian objects'.[113] Whether or not these cyber incidents are regarded as legitimate responses to Russia's aggression in Ukraine, the promotion by senior Ukrainian officials of non-state cyberattacks on civilian critical infrastructure inside Russia suggests a longer-term challenge for cyber governance. This issue could be better integrated into EU deliberations and legislation on the role of both state and non-state actors, as the current EU Policy on Cyber Defence only contains three brief references to the role of non-state actors.[114]

Means

Decoy operations

The growing use of decoy malware, combined with advanced technologies, has complicated attribution for cyber incidents, leading to mischaracterization and potential escalation. This is evident in the use of ransomware to push persistent malware as with the Bronze Starlight RATs, and of destructive malware as seen with the FoxBlade and WhisperGate wipers. Even cases involving traditional cybercrime patterns of blackmail and extortion can be complicated by the underlying geopolitical tensions. An example is the initial attribution of the DoppelPaymer case to Russia, which was later discovered to involve actors from Ukraine. Chinese and Russian interlocutors cite such cases of misattribution—alongside the limited amount of foreign attention paid to cyberattacks against their own critical infrastructure, as with NPU and Roscosmos—in voicing their own concerns over disenfranchisement.[115] While the issuance of statements and forensic reports by the Chinese government and Qihoo 360 may serve as a turning point in raising the profile of these cyber incidents, there is still a large disparity in terms of Western coverage. This combination of externally and internally inflicted opacity has contributed to Chinese and Russian alignment in establishing processes separate from those driven by the USA and the EU, and in shaping the composition of international forums to advance their distinct strategic objectives, as with the parallel Russian-sponsored OEWG and moves by China and Russia to block NGO and industry participation in international governance forums.[116] The consequences of this divergence can hinder the EU's pursuit of a cooperative global cyber governance system.

Collateral damage

Cyber incidents contribute to EU warnings of 'unacceptable risks of spillover effects, misinterpretation and possible escalation'.[117] The DoppelPaymer

[113] Maddocks, J., 'Ukraine symposium: State responsibility for non-state actors' conduct', *Articles of War*, 4 Nov. 2022.

[114] European Commission, High Representative of the Union for Foreign Affairs and Security Policy (note 2), pp. 1, 3 and 12. See also Väljataga, A., 'Cyber vigilantism in support of Ukraine: A legal analysis', NATO Cooperative Cyber Defence Centre of Excellence, Mar. 2022.

[115] Views of cybersecurity experts from China and Russia, expressed at the 'Cyber Incidents and Threat Perceptions' workshop (note 57).

[116] Cybersecurity Tech Accord (note 12); and Hurel, L. M., 'The rocky road to cyber norms at the United Nations', Council on Foreign Relations, 6 Sep. 2022.

[117] Council of the European Union, 'Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine' (note 106).

case embodies an example of the first cyber-related death. While the cyberattack violated the Fourth Geneva Convention, which explicitly prohibits attacks against civilian hospitals and medical transports, it is not an isolated occurrence.[118] Cyberattacks on critical infrastructure, whether electricity or nuclear power facilities, transportation networks, communication satellites or hospitals, still carry the chance that lives will be lost in the future. While not resulting in fatalities, the use of the AcidRain wiper against the Viasat KA-SAT, which aimed at taking down the military communication capability of Ukraine, had spillover effects that disrupted civilian services in Europe. FoxBlade malware, initially deployed to disrupt Ukraine's digital infrastructure, also affected Latvia and Lithuania.[119] Beyond civilian infrastructure, the impacted sectors are also essential for military mobility and communication, and potential cyberattacks on them could impact military assets and operations, as well as the overall defence environment in the EU.[120] Thus, while improving cyber resilience of such critical infrastructure as energy, telecommunications, transportation and space services is high on the EU's agenda, greater consideration of collateral damage that crosses national, industry and technical boundaries should factor into future EU legislation, with particular attention to better integration of both the space and cyber domains.[121]

Responses

Proactive defence

While the debate over whether EU member states should employ offensive cyber capabilities continues, the DarkSide and KillNet cyber incidents detailed above raise questions over the use of 'proactive defence' by the private sector against cyberattacks.[122] A range of cybersecurity firms have begun to emphasize the necessity of the private sector engaging in more proactive and 'zero-trust' approaches, even advocating industry to 'go on offense' in hunting for potential threats to corporate ICT networks when responding to malware campaigns.[123] While some of these recommendations are tailored to enhance proactive monitoring through cyber incident preparation, remediation and resilience, they still suggest the potential for private sector engagement in 'hack back' tactics—launching a counterattack aimed at disabling or collecting evidence against the perpetrator.[124] This in turn raises questions as to the private sector's protections under IHL, when they become enmeshed in cyber operations that blur the roles of combatant and

[118] ENISA, 'Healthcare's cybersecurity incident response spotlighted at European security event', ENISA News, 18 Nov. 2020.

[119] Brantly, A., 'From the foxhole: Cyber and kinetic conflict in Ukraine', *Cyber Defense Review*, Spring 2022.

[120] ENISA, *ENISA Threat Landscape 2022* (note 109); and European Commission, High Representative of the Union for Foreign Affairs and Security Policy (note 2).

[121] Von der Leyen, U., European Commission President, Keynote address, Tallinn Digital Summit, 10 Oct. 2022; and Raju, N. and Saalman, L., 'Space and cyberspace', in *SIPRI Yearbook 2023: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2023).

[122] Saalman, L., Su, F. and Saveleva Dovgal, L., 'Cyber posture trends in China, Russia, the United States and the European Union', SIPRI, Dec. 2022.

[123] Deloitte (note 25); and Sababa Security (note 103).

[124] Umbach, F., 'Hack-backs: Options and limitations of cyber deterrence', GIS, 7 Jan. 2021.

non-combatant.[125] An example is the collaboration between the already targeted Viasat and the US Air Force Research Laboratory on a hybrid satellite network, which promises to further diminish Viasat's civilian identity as a non-combatant.[126] Such trends are entrenched by ever-increasing delegation of responsibility and liability on the private sector under the most recent US National Cybersecurity Strategy and the 2022 update of the EU NIS Directive. Further, the EU Solidarity Act, adopted in April 2023, proposes to establish an EU Cybersecurity Reserve, which will consist of trusted and certified providers from the private sector that would be ready to intervene in cyber incidents at the request of member states.[127] While legislation that encourages private sector organizations to secure their own networks and those of state actors has merit, more consideration needs to be given to how such legislation may inadvertently encourage unauthorized offensive cyber activities and change the non-combatant status of private sector entities under IHL.

Kinetic escalation

Cyberattacks can not only render systems inoperable but can also have kinetic outcomes. Cyberattacks against assets with a dual-use nature, such as satellite systems as in the Viasat case, are particularly contentious. Russian officials have already issued threats that civilian assets used for military purposes may be targeted in the future, which could have implications for other communications platforms being assaulted with either physical or cyber means.[128] Even the use of RATs—as in the attacks against Indian aerospace firms and the PLA-affiliated NPU—can have the potential for kinetic applications in a conflict, depending on the data that has been exfiltrated. The targeting of Roscosmos by NB65 using ransomware, and a more recent false missile alert in Russia triggered by a cyberattack against media agencies in February 2023, indicate the destabilizing effects brought on by hacktivism.[129] If such cyber operations are mistaken as physical attacks, as with the NB65 claims of shutting down Roscosmos's control of its satellites or false missile attacks against Russia, they may also elicit a kinetic response. Russian officials have already stated that taking satellites offline in any country is a cause for war.[130] Missile false alarms are not new to Russia, Europe or the USA, and can trigger not only escalation, but also retaliatory strikes.[131] As the private sector expands its services using assets linked to both civilian and military operations in multiple countries, there is an increased risk of a

[125] International Committee of the Red Cross (ICRC), 'International humanitarian law and cyber operations during armed conflicts', ICRC Position Paper, Nov. 2019.

[126] Erwin (note 88).

[127] 'EU launches Cyber Solidarity Act to respond to large-scale attacks', EURACTIV, 19 Apr. 2023.

[128] Brodkin, J., 'Russian official says civilian satellites may be "legitimate" military target', *Ars Technica*, 16 Sep. 2022.

[129] Glover, C., 'Russian radio stations hacked with bogus missile warning from hacktivists', *Tech Monitor*, 23 Feb. 2023; and Burt, J., 'Kremlin claims Ukraine hackers behind fake missile strike alerts', *The Register*, 23 Feb. 2023.

[130] 'Russia space agency head says satellite hacking would justify war—report' (note 37).

[131] See e.g. The Nuclear Vault, 'False warnings of Soviet missile attacks put US Forces on alert in 1979–1980', National Security Archive, [n.d.]; and National Park Service, 'Stanislav Petrov', [n.d.]. Missile and satellite cyber incidents and related confidence-building measures will be the subject of a forthcoming SIPRI publication by the authors.

cyberattack impacting European critical infrastructure, not simply as collateral damage as in the Ukraine cases above, but also as deliberate targets.

V. Conclusions

The ongoing conflict in Ukraine has spurred a surge in malicious cyber operations aimed at the EU. This underscores the escalating complexity of cyber threats and the urgent demand for robust cybersecurity measures in the EU. The EU's traditional focus on a defence-centric regulatory system must factor in private sector responsibility for meeting these challenges, along with the concomitant demands on unifying public sector processes and consensus building within international forums.

As the EU develops these measures, four critical factors that, coupled with geopolitical tensions, may lead to escalation must be taken into consideration: (*a*) the use of decoy operations where traditional cybercrime tactics disguise cyberwarfare aims; (*b*) the growing role of hacktivists and the private sector as non-state actor combatants; (*c*) the spillover effects of cyber incidents impacting both civilian and military infrastructure; and (*d*) the potential for kinetic outcomes and responses stemming from cyberattacks on critical infrastructure. Some of the targeted responses from the private sector, public sector and international forums detailed in the case studies above can serve as a foundation for EU strategies to mitigate escalation.

Among these, most private sector responses addressed cybersecurity, but some had the potential to be escalatory and further blurred the line between state and non-state actors. For example, the direct involvement of such firms as Microsoft in the cyber defence of Ukraine not only challenges its position as a non-combatant under IHL, but also exacerbated moves by China and Russia to block NGO and industry participation in international governance forums. As a commercial sector entity already targeted by a cyberattack during the war in Ukraine, Viasat's subsequent collaboration with the US Air Force Research Laboratory on a hybrid satellite network promises to further complicate its position as a future target.

In the public sector, legislation such as the US National Cybersecurity Strategy, the 2022 update of the EU NIS Directive and the EU Solidarity Act conferred greater responsibility and liability upon the private sector to engage in cyber defence. However, there should be greater transparency about the potential fallout for private sector entities, whether they engage in state-sanctioned or unsanctioned cyber activities. In particular, the role of the non-state actor should be better integrated into the EU Policy on Cyber Defence, in light of developments such as the Ukraine government's calls for the formation of an IT Army and the potential for hacktivists to trigger kinetic escalation through cyberattacks on critical infrastructure. The transboundary nature of cyberattacks—affecting civilian and military objects across state borders and various sectors—suggests the need for better integration of both space and cyberspace legal considerations when drafting such legislation.

In terms of international forums, the action plan from the 37-member state Counter Ransomware Initiative can serve as a foundation to address the use of decoy ransomware to deliver wipers, RATs and other forms of malware for cyberwarfare. This initiative illustrates how smaller coalitions can target specific malware trends that are beyond the scope of the larger UN processes, which are increasingly difficult for NGOs and the private sector to access. It also indicates that a granular focus on combating specific malware trends can be leveraged to address not only an issue of common interest such as cybercrime, but also more contentious topics like cyberwarfare.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

SIPRI INSIGHTS ON PEACE AND SECURITY NO. 2023/09

CYBER CROSSOVER AND ITS ESCALATORY RISKS FOR EUROPE

LORA SAALMAN, FEI SU AND LARISA SAVELEVA DOVGAL

CONTENTS

ABOUT THE AUTHORS

Dr Lora Saalman (United States) is a Senior Researcher within SIPRI's Armament and Disarmament and Conflict, Peace and Security research areas.

Fei Su (China) is a Researcher with SIPRI's China and Asia Security Programme.

Larisa Saveleva Dovgal (Russia) is a Research Assistant with the SIPRI Weapons of Mass Destruction Programme.