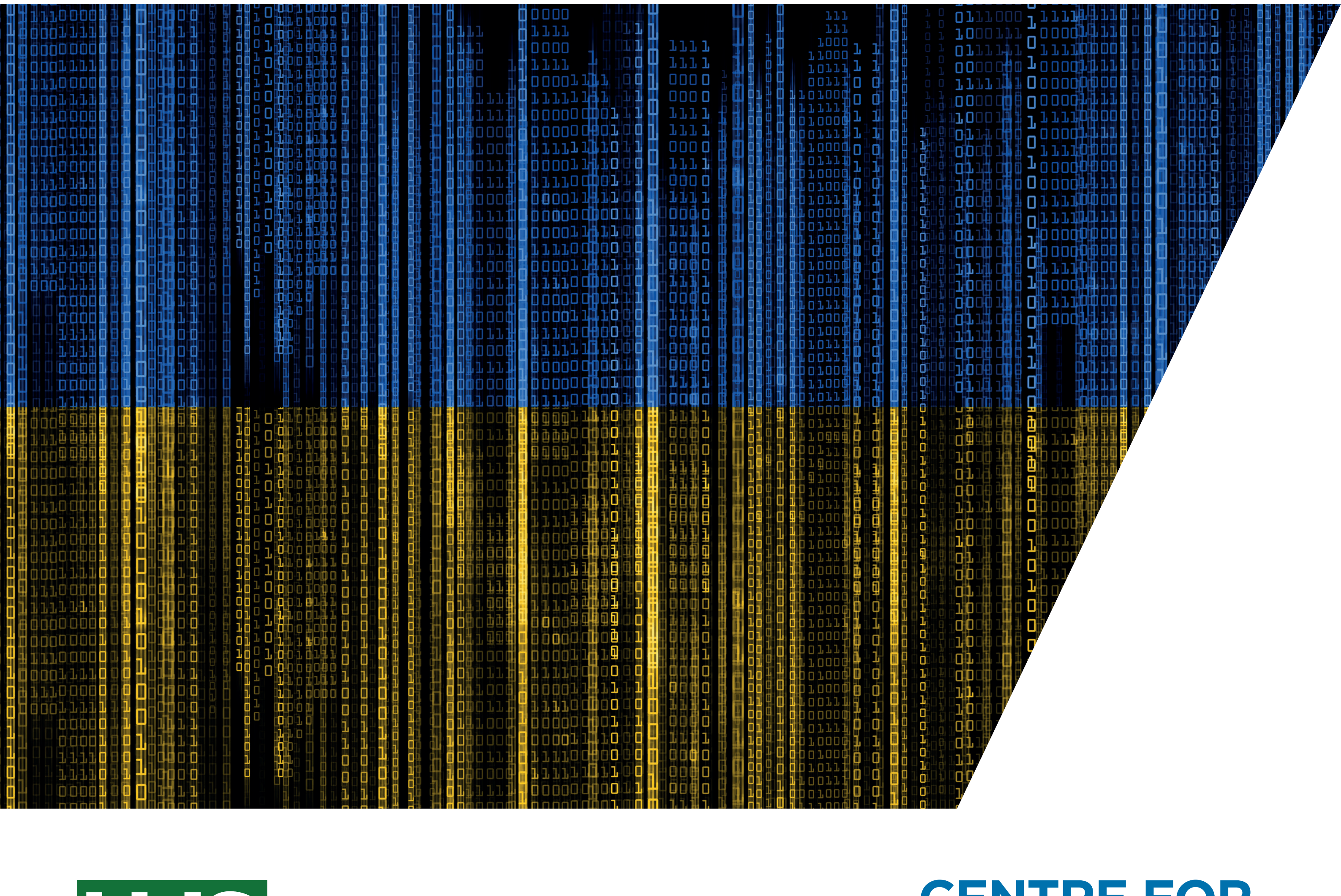
LESSONS FROM THE FIRST CYBER WAR: HOW SUPPORTING UKRAINE ON THE DIGITAL BATTLEFIELD CAN HELP IMPROVE THE UK'S ONLINE RESILIENCE

BY DAVID KIRICHENKO



HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RUSSIA AND EURASIA STUDIES

February 2024

Published in 2024 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

Title: “LESSONS FROM THE FIRST CYBER WAR: HOW SUPPORTING UKRAINE ON THE DIGITAL BATTLEFIELD CAN HELP IMPROVE THE UK’S ONLINE RESILIENCE”
By David Kirichenko

ISBN: 978-1-909035-90-4

£9.95 where sold

The views expressed in this publication are those of the author and are not necessarily indicative of those of The Henry Jackson Society or its Trustees.

Cover image: Binary code pattern in the colours of the Ukrainian flag by Ground Picture at Shutterstock (https://www.shutterstock.com/image-photo/technology-cyberspace-information-concept-binary-code-2133310075).

LESSONS FROM THE FIRST CYBER WAR: HOW SUPPORTING UKRAINE ON THE DIGITAL BATTLEFIELD CAN HELP IMPROVE THE UK'S ONLINE RESILIENCE

BY DAVID KIRICHENKO

HJS
Henry
Jackson
Society

CENTRE FOR RUSSIA AND EURASIA STUDIES

DEMOCRACY | FREEDOM | HUMAN RIGHTS

February 2024

About the Author

David Kirichenko is a researcher and expert specialising in the fields of cyber warfare and irregular warfare. His analysis is widely published in outlets such as the Atlantic Council, Center for European Policy Analysis, Irregular Warfare Center, and The Hill, as well as in peer-reviewed journals. His writing has been cited in journals such as the Journal of Advanced Military Studies and the Asymmetric Threat Analysis Center at the University of Maryland, among others. David has worked in the field of security engineering, focusing on building threat detections, utilising open-source software, and managing vulnerabilities.

Acknowledgments

The author wishes to express his profound gratitude to Bryan Larish, PhD and Treston Wheat, PhD for their invaluable contributions in reviewing various versions of this report.

Additionally, heartfelt thanks are extended to the entire team at the Henry Jackson Society for providing both the opportunity to undertake this project and the essential support needed to bring it to fruition.

Contents

About Us

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances which keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

CENTRE FOR
RUSSIA AND
EURASIA
STUDIES

About the Centre for Russia and Eurasia Studies

The **Centre for Russia and Eurasia Studies** undertakes in-depth, analytically-focussed research into domestic and foreign policy issues in Russia and the other post-Soviet states. Established in 2010 as the Russia Studies Centre, the programme's geographical scope has widened since 2014, mirroring the high level of importance attached to the region.

Executive Summary

Russia’s full-scale invasion of Ukraine triggered the largest war in Europe since World War II. The invasion also marked the first all-out cyber war between two nation-states, as Russia attempted to integrate cyberattacks with physical strikes. Ukrainian digital infrastructure and systems were put to the test against what many experts previously feared would be a “digital Pearl Harbor”. Just as Ukraine's valiant resistance on the battlefield took the world by surprise in the early days of the war, its cyber defences also stood firm, successfully weathering the initial cyber onslaught.

Russian attempts to secure cyber victories early on were largely thwarted, with disruptions to Ukraine's military satellite provider, Viasat, proving only temporary and having minimal impact. Ukraine used its extensive experience from Russia’s initial invasion in 2014 to prepare for the full-scale invasion in 2022, both on the cyber and physical fronts. What was different about the cyber defences was not only the important role that Western governments played in strengthening Ukraine’s defences, but the increasingly important role that Western tech companies would play. Cyber warfare is also becoming decentralised and crowdsourced as both Ukraine and Russia look to non-state actors to support cyber campaigns and the growing role of civilians.

The West must reframe its thinking about how it supports Ukraine and helps to improve Ukraine’s capabilities to conduct a larger cyber offensive against Russia in support of its battlefield objectives. Russia’s cyber war against Ukraine and the West is part of its wider campaign to prevail on the physical front and destroy Ukraine before moving further West. Keeping Ukraine alive in the fight and supporting its defence won’t bring victory and peace, but giving Ukraine the abilities and means to win on the digital and physical fronts will protect the Western world. Given how interconnected the world is through the internet and our digitised societies, protecting Ukraine’s network would also mean the West was protecting its own network, as was seen in the devastating NotPetya attacks in 2017.

Furthermore, as Western tech companies depart from Russia and Russia is forced to leverage Chinese or domestic tech, the opportunities for Ukraine to conduct more devastating cyberattacks will expand. Helping Ukraine wage these cyberattacks will help the West learn more about how these weapons can be used in future conflicts and how to improve cyber defences against certain exploits. Furthermore, the UK should take lessons from Russia’s cyber aggression and how it has exposed vulnerabilities in critical infrastructure. These lessons will inform how to improve cyber defences and ensure robust processes are in place for the private and public sectors to work closely in the event of a future cyber war.

In supporting Ukraine on the digital battlefield, the UK should:

1. Improve coordination between the private and public sectors for shoring up cyber defences;
2. Invest in creating stronger security mechanisms to protect critical infrastructure;
3. Continue to provide support for Ukraine’s cyber defence;
4. Provide Ukraine with more intelligence on Russian vulnerabilities to enable Ukraine to conduct cyber offensives to support its ground campaign; and
5. Begin expanding “Hunt Forward” operations with allied nations that are under potential threat.

Introduction

As Russian tanks began rolling into Ukraine and bombs fell across the country in February 2022, Europe bore witness to the largest conflict on European soil since World War II. However, Russia's invasion of Ukraine wasn't limited to physical operations; it also marked the start of the first all-out cyber war. It is important for the West to quickly study the lessons learned so far from this cyber war between Russia and Ukraine. Additionally, it is crucial to help the Ukrainians expand their capabilities on the cyber front, just as military assistance is needed on the physical battlefield. By applying these lessons, the UK and the West can strengthen their cyber defences and better prepare allies, such as Taiwan, for future cyber conflicts.

As the world became digitised and the Kremlin grew in its revisionist ambitions, Russia began using cyberattacks as a new tool to achieve its political aims. Starting in Estonia in 2007 to punish the country for what it deemed anti-Russia behaviour, Russia then waged cyberattacks against Georgia to accompany its physical attack on the country. It used Ukraine as a testing ground for cyber weapons before ultimately beginning the first all-out cyber war against Ukraine in February 2022. While Ukraine survived many of the most devastating attacks on critical infrastructure, the cyber war between Israel and Iran has also shown the extremes that these attacks can go to, such as the attack on Iran's nuclear power plant.

While a successful coalition of Western governments and tech companies has played a vital role in keeping Ukraine's cyber defences resilient, much like on the physical battlefield, without offensive support, Ukraine is limited in its ability to match and overwhelm Russian cyberattacks. At the start of the invasion, Russia attempted to knock out vital communication systems for the Ukrainian military with an attack on Viasat satellites, marking its most damaging attack of the war so far on Ukraine's telecom provider, Kyivstar. The intensity of the Russian cyberattacks is growing as the war drags on, and Ukraine should be armed to degrade Russia's offensive cyber capabilities. Destroying the enemy's ability to wage war is a key principle in warfare, whether conventional or cyber.

Giving support on cyber capabilities is important now because this is the first war with integrated cyber and physical strikes on the battlefield and there are many lessons to learn for future wars. While Russia has not integrated both well, Ukraine should be given more opportunities to execute properly with Western backing.

If the West fails to properly support Ukraine in this cyber war, it will also undermine its own ability to fight on the battlefield in the future. It further undermines the West's investment in conventional armaments if physical operations are not supported by cyber. What happens on the cyber front isn't merely related to Ukraine and Russia, but has a direct impact on the West because Russia has already been waging hybrid warfare for years. As cyber remains a grey area, Russia will continue to increase its attacks on the West, especially as the world becomes even more digitally dependent. Thus, reinforcing Ukraine's cyber capabilities not only addresses immediate threats but also strategically curbs Russia's capabilities.

It is in the interests of the West to help give Ukraine the cyber weaponry that is needed to achieve the West's security interests. This includes sharing, prior to public disclosure, information on zero-day vulnerabilities – known to Western technology firms and intelligence agencies – with Ukraine. Such intelligence sharing would enable Ukraine to strategically target Russia's economic and infrastructural capacities, undermining its war efforts.[1] Tech companies

[1] A zero-day vulnerability is a software security flaw that can be exploited by attackers before the developer has had a chance to create and release a patch or fix, leaving users vulnerable and unprotected.

and governments in the West should carefully assess the risks and, where suitable, contemplate supplying intelligence to Ukraine. Moreover, as Western tech companies increasingly withdraw from Russia, the opportunity for action will expand. Russia will be compelled to rely more heavily on its internal technology resources, thereby reducing the potential for collateral damage to the West from exploiting vulnerabilities in Russian systems.

Giving Ukraine the right vulnerabilities to exploit will also provide the West with an opportunity to study what is most effective in cyber war and to improve the West's own cyber defences. Finally, assisting Ukraine's cyber defence will help to begin defining cyber red lines for NATO which do not exist as Russia continues to push the boundaries and attack critical infrastructure. If Ukraine is able to wage larger-scale cyber campaigns against Russia with Western support effectively, it could serve to deter other nation states like China, Iran and North Korea from launching devastating cyberattacks in the future.

I. Prelude to the Russo–Ukrainian War

In July 2021, a year prior to the full-scale invasion of Ukraine, Russian President Vladimir Putin authored a lengthy 6000-word essay titled 'On the Historical Unity of Russians and Ukrainians'.[2] This document presented a stark and threatening perspective: the paper argued that Ukraine's lack of a unique identity actually made it an integral part of the Russian ethnos; it framed Ukraine as an artificially constructed state on land that historically belongs to Russia; and it denied the legitimacy of Ukrainian nationhood and sovereignty apart from Russia. These assertions were not isolated; Putin reiterated them in various key speeches, including his declaration of war on 21 February 2022.[3]

Russian Foreign Minister Sergey Lavrov once noted that Putin's guidance comes from three historical figures: Ivan the Terrible, Peter the Great and Catherine the Great.[4] Putin's emulation of Peter the Great is particularly revealing, underscoring his ambition to reclaim territories he deems rightfully Russian. Drawing parallels with Peter's 18th-century campaigns against Sweden, Putin casts his actions as a restoration of Russian lands rather than territorial expansion.[5]

At the core of the Kremlin's narrative is the concept of the "divided Russian people", with Ukraine, especially Kyiv – the cradle of Russian civilisation in Russia's view – seen as a significant symbolic and territorial loss that must be reclaimed.[6] This mindset fuels Russia's territorial ambitions in Ukraine. In 2008, Putin lectured then-US President George W. Bush that Ukraine wasn't a legitimate state.[7] Echoing the perspectives of Russian tsars and Stalin, Putin views the statehood and national identity of Ukraine as impediments to Russia's imperial ambitions. It also shows that Russia has no intention of stopping the war until it has fully subjugated Ukraine. All losses of money, men and equipment are rationalised because of the mindset of entitlement that possesses the Russian elite. In December 2023, Putin insisted that there would be no peace until Russia achieves its goals.[8]

In January 2024, Latvian Foreign Minister Krišjānis Kariņš stated that Russia's war of aggression wouldn't end even after it had finished with Ukraine. He believes NATO needs a long-term containment plan for Russia.[9] Belgian army chief Michel Hofman also highlighted that Russia will likely attack the Baltics and Moldova after Ukraine.[10] However, NATO also needs to consider that it requires a containment plan not only for the physical battlefield in Ukraine, but also for

[2] Vladimir Putin, "On the Historical Unity of Russians and Ukrainians", President of Russia, 12 July 2021, http://en.kremlin.ru/events/president/news/66181.

[3] "'No Other Option': Excerpts of Putin's Speech declaring war", Al Jazeera, 24 February 2022, https://www.aljazeera.com/news/2022/2/24/putins-speech-declaring-war-on-ukraine-translated-excerpts.

[4] Timothy Garton Ash, "Putin, Pushkin, and the decline of the Russian empire", ECFR, 23 August 2023, https://ecfr.eu/article/putin-pushkin-and-the-decline-of-the-russian-empire/.

[5] Andrew Roth, "Putin compares himself to Peter the Great in quest to take back Russian lands", The Guardian, 10 June 2022, https://www.theguardian.com/world/2022/jun/10/putin-compares-himself-to-peter-the-great-in-quest-to-take-back-russian-lands.

[6] Igor Torbakov, "Deadly Illusions: The Ukraine War and Russian Historical Imagination", The Russia Program, May 2023, https://therussiaprogram.org/onlinepaper_3.

[7] Daniel Baer, "Ukraine's not a country, Putin told Bush. What'd he tell Trump about Montenegro?", The Washington Post, 19 July 2018, https://www.washingtonpost.com/news/posteverything/wp/2018/07/19/ukraines-not-a-country-putin-told-bush-whatd-he-tell-trump-about-montenegro/.

[8] Harriet Morris, "An emboldened, confident Putin says there will be no peace in Ukraine until Russia's goals are met", AP News, 14 December 2023, https://apnews.com/article/putin-russia-press-conference-moscow-ukraine-ef4e88fda50e6ad75b8a1979b95d9fcc.

[9] Claudia Chiappa, "Russia 'will not stop' at Ukraine, Latvia warns", POLITICO, 5 January 2024, https://www.politico.eu/article/krisjanis-karins-russia-will-not-stop-ukraine-latvia-war/.

[10] Laura Hülsemann, "Putin could attack Baltics and Moldova next, says Belgian army Chief", POLITICO, 19 December 2023, https://www.politico.eu/article/belgian-army-chief-hofman-putin-attack-after-ukraine-baltics-moldova-next-russia/.

Russia's cyber aggression. Therefore, for both the physical and cyber realms, it is important to understand that Russia has no intention of stopping any time soon and that the best course of action is to give Ukraine what it needs to win.

Understanding the Kremlin's motivations is crucial for shaping the West's policies on aiding Ukraine as Moscow aims to subjugate the Ukrainian people and ensure the country remains under Russia's domination. A free Ukraine will always serve to threaten an authoritarian Russia. As long as the West continues to protect the European continent from Russian imperialism and supports Ukraine's fight, Russia will continue to wage cyber war on both Ukraine and the West.

II. Cyber Warfare Theory

As the internet connects more people, businesses, governments and military systems, it also becomes a gateway for cyberattacks. National infrastructures, government systems and financial institutions, all linked by networks, are at risk. The growing number of potential cyberattack vectors means that ordinary citizens can also become involved in waging cyber warfare, like Ukraine's volunteer IT Army, or they could become targets.

The 19th-century wartime strategist Carl von Clausewitz defined war as "an act of force to compel our enemy to do our will".[11] This perspective also views war as a state-directed effort to achieve political objectives. Central to his theory is the 'warfare trinity' of the people, the military, and the government. Historically, this trinity operated in the physical realm, predominantly through physical force – a characteristic of the industrial age. Clausewitz argued that, while the nature of war remains constant, its manifestation evolves over time with advancements in technology.

In the transition to the information age, the principles of Clausewitz's warfare trinity remain relevant, but the battlefield has transformed. Cyber warfare now represents a new domain where physical force is replaced by information and digital tools. This form of warfare simultaneously impacts all aspects of the trinity – people, military and government – almost instantaneously, and often with global scope. The rise of cyber warfare illustrates Clausewitz's belief that the nature of war is immutable, but the methods and arenas of warfare continue to evolve.

Today, cyber warfare aims to achieve political and strategic objectives through cyberspace, extending the battleground beyond physical spaces. It blurs traditional lines between combatants and non-combatants, as civilians can both willingly and unwittingly become part of cyber conflicts. Russia also uses organised crime for cyber operations against the West. In the past, there was also a clear difference between civilians and soldiers, often marked by uniforms. Civilians were usually away from the battlefield, which had defined boundaries. However, in modern conflicts, this distinction has faded. Today's enemies often include non-state actors who blend in with civilians, making it hard to tell them apart, and the concept of a specific battlefield has vanished; military actions can now happen anywhere.

Cyber Norms and International Agreements

As the internet interconnects more facets of our lives, it opens up new arenas for nation-states waging war, making the establishment of international cyber norms and agreements more relevant. The shift from traditional battlefields to cyber warfare necessitates a re-evaluation of how international law and wartime strategies apply to the digital domain due to the increasing involvement of civilians in cyber conflicts and the blurring of lines between combatants and non-combatants. Initiatives like the Tallinn Manual and the Red Cross cyber norms have emerged as critical efforts to adapt existing legal frameworks to the realities of cyber warfare, aiming to mitigate the impact on civilians and ensure a degree of accountability and restraint in cyberspace.

a) Tallinn Agreement

This agreement stems from the work done in the Tallinn Manual, an influential guide on how international law applies to cyber warfare. The Tallinn Manual, initiated by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, was developed by an international group of legal scholars and practitioners. It has become an influential resource for scholars and policymakers to use as a framework to deal with cyber warfare.[12] The Tallinn Agreement

[11] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), p.149.

[12] "The Tallinn Manual", https://ccdcoe.org/research/tallinn-manual/.

was created following Russia's first large-scale cyberattack against Estonia in 2007.[13] The process began in 2009 when the NATO CCDCOE recognised the growing importance and unique challenges of cyber operations in international law and initiated a project to clarify the legal landscape. The necessity for such a manual became clear due to the growing incidence of cyber operations that potentially crossed the line into armed conflict, or at least had significant international legal implications. The manual addresses issues like sovereignty, state responsibility, the applicability of international humanitarian law in cyberspace, and the conduct of hostilities.

The first version, known as Tallinn Manual 1.0, was published in 2013 and focused specifically on the most severe forms of cyber operations – those that would be considered equivalent to armed attacks under international law and the laws of armed conflict.[14] Tallinn Manual 2.0, published in 2017, expanded this scope to include a broader range of cyber operations, especially those occurring outside the context of armed conflict.[15] This included considerations of sovereignty, state responsibility and human rights.

b) Red Cross Cyber Norms

The International Committee of the Red Cross (ICRC) has been advocating for the application of existing international humanitarian law to cyber warfare, especially emphasising the need to protect civilians and civilian infrastructure. One theme that has featured prominently in the Russo–Ukrainian war has been the rise of civilians engaging in digital warfare.[16] Some of these civilians are minors, which may complicate the classification of them as enemy combatants in the cyber realm. The Red Cross cyber norms seek to clarify how principles like distinction, proportionality and necessity apply in the digital sphere, particularly given the potential for significant civilian harm due to cyber operations targeting critical infrastructure like hospitals, power grids and water systems. Like the Tallinn Manual, the ICRC's positions on cyber operations are interpretative, advisory and are non-binding. They don't create new legal obligations but aim to influence states and other actors to consider humanitarian principles when engaging in cyber warfare.

As countries like Russia expanded their efforts to conduct cyber warfare against other countries, the need to create international norms and frameworks began to take shape. However, even as these agreements and frameworks were being created, Russian attacks against the West and Ukraine became more brazen and destructive, with many of Russia's attacks in recent years targeting critical infrastructure.

[13] Stephanie MacLellan and Naomi O'Leary, "Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game", Centre for International Governance Innovation, 26 October 2017, https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game/.

[14] Michael J. Adams, "A Warning about Tallinn 2.0 … Whatever It Says", The Lawfare Institute, 4 January 2017, https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says.

[15] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", *Georgetown Journal of International Law*, 15 March 2017, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

[16] Tilman Rodenhäuser and Mauro Vignati, "8 Rules for 'Civilian Hackers' during war, and 4 obligations for states to restrain them", Humanitarian Law & Policy Blog, 4 October 2023, https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.

III. Case Studies of Cyber in War

Over the past two decades, warfare has expanded beyond mere physical confrontations to encompass the digital realm. As a result, cyber capabilities have been growing, leading nation-states like Israel and Russia to increasingly utilise cyberattacks in support of their political objectives. A comparison of the cyberattacks on Estonia in 2007 with the complex cyber operations against Ukraine up to 2022 provides insight into how Russia has conducted its cyber campaigns in the past, how its capabilities have evolved, and how cyber strategies support political goals.

Cyberattacks Before 2022

a) Estonia 2007

In the spring of 2007, Estonia experienced what came to be known as the first cyberattack on a nation-state.[17] This campaign was linked to a wider political dispute with Russia over the relocation of a Soviet-era monument in Tallinn. The cyberattacks, which began on 27 April, targeted Estonia's internet infrastructure, including banks, media outlets and government services.

The cyberattacks were mostly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. They overwhelmed servers with massive waves of network traffic, sent from botnets and automated requests, disrupting online services at an unprecedented level.[18] Estonia's experience was the first instance of a nation facing this modern form of hybrid warfare. The effectiveness of the Russian cyberattacks on Estonia was amplified due to the country's extensive reliance on the internet. In 2000, Estonia's parliament had even declared internet access a human right, and the country has invested heavily into digitisation.[19] These attacks flagged the vulnerabilities in a highly digitised society, demonstrating the risks of embracing extensive digitalisation.

The attacks demonstrated that cyber warfare is a serious tool for societal disruption in military contexts as it can cause damage, but also not be followed with any sort of military retaliation. Following the attack, Estonia established a voluntary Cyber Defence Unit – something that Ukraine is currently considering as well.[20]

A notable aspect of these attacks was their ambiguity as the attacks were conducted by a wide variety of actors including cyber gangs loyal to Moscow.[21] This allows any state sponsor orchestrating the attacks to remain hidden and deny involvement, as attribution is difficult without proving who is responsible, which is incredibly difficult in cyberspace. The 2007 attack on Estonia also helped to speed up the creation of the NATO CCDCOE in 2008.[22] It became NATO's cyber defence centre, which today includes over 30 NATO members, with Ukraine having joined the centre in 2023.[23]

[17] Damien McGuinness, "How a cyber attack transformed Estonia", *BBC News*, 27 April 2017, https://www.bbc.com/news/39655415.

[18] James Pamment, et al., "Hybrid Threats: 2007 cyber attacks on Estonia", NATO Strategic Communications Centre of Excellence, 6 June 2019, https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

[19] Imtiaz Khan and Ali Shahaab, "Estonia is a 'digital republic' – what that means and why it may be everyone's future", *The Conversation*, 7 October 2020, https://theconversation.com/estonia-is-a-digital-republic-what-that-means-and-why-it-may-be-everyones-future-145485.

[20] William Casey Biggerstaff, "The status of Ukraine's 'IT Army' under the law of armed conflict", Lieber Institute West Point, 10 May 2023, https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/.

[21] Mark Galeotti, "Crimintern: How the Kremlin uses Russia's criminal networks in Europe", ECFR, 18 April 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[22] "NATO CCDCOE – Expertise and cooperation make our cyber space safer", e-Estonia, 16 October 2018, https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/.

[23] Alexander Martin, "Ukraine, Ireland, Iceland and Japan officially join NATO's cyber defense center", *The Record*, 17 May 2023, https://therecord.media/nato-ccdcoe-ukraine-iceland-ireland-japan.

b) The Russo–Georgia War of 2008

In August 2008, during its invasion of Georgia, Russia combined cyberattacks with military actions on the ground. This was the first time such a coordinated effort had been seen in warfare. This Russian–Georgian war stemmed from frozen Russian-controlled conflicts in Abkhazia and South Ossetia, which Georgian President Mikhail Saakashvili sought to end.

This early form of cyber warfare was characterised by its alignment with Russia's military and political objectives, contrasting with the earlier 2007 Estonia cyber incident. Russia's strategy focused on controlling Georgian military and government communication channels. Prior to Russia's physical invasion, Georgian government sites experienced a pre-emptive cyberattack that began on 20 July 2008; the website of the president was overwhelmed by traffic, including the phrase "win+love+in+Russia", and was inoperable for 24 hours. [24]

The attacks intensified on 8 August, with a series of DDoS attacks coinciding with Russia's invasion of South Ossetia. [25] These cyberattacks had effectively disabled most of Georgia's governmental websites by 10 August. Faced with a communication blackout, Georgia sought cyber refuge by relocating critical official internet assets to the United States, Estonia, and Poland without prior US Government approval. [26]

The primary objective of the Russian cyberattacks on Georgia was to isolate and silence the country. [27] This strategy also included disrupting Georgian banks, which faced a deluge of fraudulent transactions, prompting international banks to halt their operations in Georgia to limit damage. Consequently, Georgia's banking system was incapacitated for 10 days. This disruption extended to the shutdown of mobile phone services, further severing Georgia's communication with the outside world.

Russian hackers also took aim at Georgian commercial websites, causing economic damage akin to the disruption experienced by the banking system. During the attacks, 35% of Georgia's internet networks experienced reduced functionality, peaking during the Russian invasion of South Ossetia between 8 and 10 August. [28]

In response to the cyber onslaught, Georgia initially tried filtering Russian IP addresses. However, Russian hackers quickly adapted, employing non-Russian servers and spoofed IP addresses to continue their attacks. [29] This series of events demonstrated Russia's ability to effectively integrate cyber warfare with conventional military operations, achieving its strategic goals and setting a precedent for future conflicts. Russia's cyber offensive also demonstrated the importance of protecting not only military networks, but also civilian computer networks.

The attacks catalysed expert discussions about the concept of a "digital Pearl Harbor", a scenario where a nation's infrastructure is overwhelmed and shut down through internet-based attacks. Many also predicted that Russia's 2022 invasion of Ukraine would unleash a "digital Pearl Harbor".

[24] John Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*, 12 August 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html.

[25] Siobhan Gorman, "Georgia States Computers Hit By Cyberattack", *The Wall Street Journal*, 12 August 2008, https://www.wsj.com/articles/SB121850756472932159.

[26] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook", *Parameters* 38, no.4 (2008), doi:10.55540/0031-1723.2455.

[27] Paulo Shakarian, "The 2008 Russian Cyber-Campaign Against Georgia", *Military Review*, January 2011, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf.

[28] Sarah P. White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War", Modern War Institute, 20 March 2018, https://mwi.westpoint.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

[29] Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war", *Security Dialogue* 43, no.1 (2012): 3–24, http://www.jstor.org/stable/26301960.

c) Kyrgyzstan 2009

In January 2009, Kyrgyzstan hosted an American military base, the Manas Air Base, which played a strategic role in US military operations in Afghanistan.[30] Russia, seeking to expand its sphere of influence in Central Asia, wanted to reduce the American presence in the region, and was negotiating with the Kyrgyz Government over the air base. While negotiations were underway, Russian hackers carried out a DDoS attack against Kyrgyzstan. The attack took out two of Kyrgyzstan's four main internet service providers, which were shut down due to the attack.[31]

The cyberattack was part of a broader strategy by Russia to pressure the Kyrgyz Government as it coincided with negotiations and discussions regarding the American military base. Following the cyberattack, and amidst ongoing negotiations, Kyrgyzstan announced its decision to shut down the American military base.[32] Russia's 2009 cyberattack on Kyrgyzstan continued to demonstrate to the Russian leadership the growing role of cyber capabilities as tools of statecraft and how it could be used to threaten or strong-arm countries.

d) Israel–Iran Cyber War (2010 – Present)

Since the 1979 Islamic Revolution in Iran, there has been a four-decade conflict between Iran and Israel. The revolution ushered in a new Islamic regime in Iran, which adopted the Palestinian cause and severed diplomatic ties with Israel.[33] The rivalry extended beyond direct confrontation to a proxy war, with Iran supporting terrorist groups like Hezbollah in Lebanon and Hamas in Gaza, both of which border Israel. However, the proxy war would eventually extend into a direct conflict between Iran and Israel in cyber space.

Cyber warfare had become a new front in this conflict by 2010, although the extent remains largely undisclosed, as neither nation openly admits to launching cyberattacks against the other. Israel, often in collaboration with the United States, is suspected of conducting several sophisticated cyber operations targeting Iran's nuclear programme.[34] The most notable attack in the cyber war was the discovery of the Stuxnet virus in Iran's Bushehr nuclear power plant computers in 2010.[35] Believed to be a joint creation of Israel and the United States through Operation Olympic Games, Stuxnet was engineered to cause physical damage by speeding up and destroying the IR-1 centrifuges, leading to the destruction of about 1000 out of 9000 centrifuges at Natanz.[36] Stuxnet effectively disrupted production at Natanz by damaging the facility's equipment. Iran attributed this attack to Israel and the United States.[37]

In response to the Stuxnet incident, Iran significantly bolstered its cyber capabilities, enhancing both defensive and offensive measures.[38] Between 2012 and 2015, Iran's cyber security budget

[30] "US Transit Center at Manas", NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/manas_transit_center.pdf.

[31] Nathan Hodge, "Russian 'cyber Militia' Takes Kyrgyzstan Offline?", *Wired*, 28 January 2009, https://www.wired.com/2009/01/cyber-militia-t/.

[32] Olga Dzyubenko, "Kyrgyzstan says U.S. base decision is final", *Reuters*, 6 February 2009, https://www.reuters.com/article/idUSTRE5151FI/.

[33] Maziar Motamedi, "Iran and Israel: From allies to archenemies, how did they get here?", *Al Jazeera*, 6 November 2023, https://www.aljazeera.com/news/2023/11/6/iran-and-israel-from-allies-to-archenemies-how-did-they-get-here.

[34] Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say", *The Washington Post*, 2 June 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[35] Bruce Schneier, "The Story Behind The Stuxnet Virus", *Forbes*, 7 October, 2010, https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html?sh=2a4b411851e8.

[36] "Report: Iran Accelerates Cyberattacks", United States Institute of Peace, 31 July 2023, https://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks.

[37] "Iran blames U.S., Israel for Stuxnet malware", *CBS News*, 16 April 2011, https://www.cbsnews.com/news/iran-blames-us-israel-for-stuxnet-malware/.

[38] Andrea Shalal-Esa, "Iran strengthened cyber capabilities after Stuxnet: U.S. general", *Reuters*, 18 January 2013, https://www.reuters.com/article/idUSBRE90G1C4/.

increased around 1200% and, after Stuxnet, Iran began focusing the majority of its cyber espionage against Israel.[39] At a 2019 tech conference, Israeli Prime Minister Benjamin Netanyahu claimed that Iran was constantly conducting cyberattacks that targeted Israel's critical infrastructure.[40]

In April 2020, Israel experienced a cyberattack on its water and sewer facilities, leading to temporary disruptions in local water systems. Initially attributed to a technical malfunction by the Israeli Government, it was later identified as an attack by Iran. In response, Israel launched a retaliatory cyberattack the following month against the Shahid Rajee Port, targeting the operating systems of private shipping companies. The consequences were widespread, causing prolonged road and waterway congestion.[41]

The Iranian attack on Israel was believed to have been targeting the water supply by increasing chlorine in the water that is delivered to residential areas.[42] Yigal Unna, the head of Israel's National Cyber Directorate, believed that if the attack had not been detected in time, chlorine or other chemicals could have been mixed into the water supply, poisoning many civilians.[43]

In 2021, Israel was accused by Iran of conducting a cyberattack that took down many of the country's gas stations by sabotaging a payment system, leaving many people unable to buy petrol for their vehicles.[44]

While nations routinely engage in probing each other's public utilities to identify vulnerabilities and establish a persistent presence, the escalation to actual attacks is a rarity. But if nation-states really did want to execute large-scale cyberattacks against civilian infrastructure, the consequences could be deadly for the civilian populations.

e) Russian Cyber Operations Against Ukraine (2014–2022)

From the Estonian attack in 2007 to leveraging cyber operations and supporting military operations in Georgia in 2008, Russia already had some experience waging cyber war. However, before the Euromaidan Revolution in Ukraine in late November 2013, Russia had begun preparing for an actual war against Ukraine – both physical and digital. Ukraine's president at the time, Viktor Yanukovych, who had close ties with Russia, had backpedalled against closer ties with the European Union, refusing under the Kremlin's pressure to sign an Association Agreement with the EU.[45]

Russia offered Ukraine US$15 billion in economic aid, which was seen as a bribe to Yanukovych to turn away from the EU.[46] Activists started large protests against the president's decision to try and bring the country deeper into Russia's sphere of influence. Yanukovych tried to stop these protests with force, but that only made the protesters more determined and

[39] Ashish Kumar Sen, "Iran's Growing Cyber Capabilities in a Post-Stuxnet Era", *Atlantic Council*, 10 April 2015, https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/.

[40] Shoshanna Solomon, "Iran attacks Israel in cybersphere 'daily,' Netanyahu charges", *Times of Israel*, 29 January 2019, https://www.timesofisrael.com/iran-attacks-israel-in-cybersphere-daily-netanyahu-charges/.

[41] Wei Chieh Lim, "Hidden Cyber War between Israel and Iran Spills Into Public View With Attacks on Physical Infrastructure", *CPO Magazine*, 19 June 2020, https://www.cpomagazine.com/cyber-security/hidden-cyber-war-between-israel-and-iran-spills-into-public-view-with-attacks-on-physical-infrastructure/.

[42] "Cyber attacks again hit Israel's water system, shutting agricultural pumps", *Times of Israel*, 17 July 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.

[43] "'Cyber winter is coming,' warns Israel cyber chief after attack on water systems", *Times of Israel*, 28 May 2020, https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/.

[44] Vivian Yee, "Iranian Motorists Hit with Cyberattack at Filling Stations", *The New York Times*, 26 October 2021, https://www.nytimes.com/2021/10/26/world/middleeast/iran-gas-station-hack.html.

[45] Oksana Grytsenko and Ian Traynor, "Ukraine U-turn on Europe pact was agreed with Vladimir Putin", *The Guardian*, 26 November 2013, https://www.theguardian.com/world/2013/nov/26/ukraine-u-turn-eu-pact-putin.

[46] Elizabeth Piper, "Special Report: Why Ukraine spurned the EU and embraced Russia", *Reuters*, 19 December 2013, https://www.reuters.com/article/idUSBRE9BI0E2/.

brought more people into the streets. The situation continued to escalate, and eventually Yanukovych fled to Russia. Putin exerted pressure on Yanukovych to pivot Ukraine towards joining the Eurasian Economic Union (EEU), mirroring Russia's successful coercion of Armenia. Unlike Armenia's transition from the EU Association Agreement to the EEU, which occurred without significant public dissent, Ukraine's situation was markedly different, culminating in mass protests. Following the ascent of the Euromaidan activists to power, Russia executed an invasion of Crimea. This operation was characterised by the deployment of Russian special forces, who were notably disguised as 'little green men' – soldiers without identifiable insignia. [47, 48]

However, during Russia's invasion of Crimea and illegal referendum, the Kremlin also launched an eight-minute DDoS attack against Ukraine, which was 32 times more powerful than Russia's largest attack against Georgia during its invasion in 2008. [49] Then on the day of the illegal referendum in Crimea, Russia also began conducting DDoS attacks against NATO websites for voicing support for Ukraine against Russia's invasion. [50] This set a precedent for Russia targeting supporters of Ukraine with cyberattacks in subsequent confrontations.

In May 2014, the pro-Russian hacktivist group CyberBerkut tried to disrupt the Ukrainian presidential elections. Four days before the vote, they hacked into Ukraine's main election computers and deleted important files, causing the system that counts the votes to stop working. The next day, the hackers announced they had "destroyed the computer network infrastructure" used for the election, leaking emails and documents online to show what they had done. Furthermore, they continued attacking the vote counting system with DDoS attacks, which overloaded the system with traffic. The next day, Ukrainian officials reported that they had fixed the system by using backup files, and it was ready to be used again. However, government cyber experts still had to remove a virus 40 minutes before the results were announced which would have resulted in false votes being released. [51]

Russia's aim was to discredit Ukraine's elections. The attacks also revealed how Russian cyber operations are targeted to disrupt services and create instability. [52] In April 2014, after illegally annexing Crimea, Russia also sent militant groups into south-eastern Ukraine to create a violent uprising which ultimately led to war in Ukraine's Eastern Donbas region between Ukraine and Russian-backed militants. [53]

As Russian tanks invaded Ukraine in August 2014, Russian hackers were already working on conducting cyberattacks against Ukraine, with the country distracted by what was happening politically. [54] The war in eastern Ukraine also gave Russian-affiliated hackers the opportunity to

[47] Steven Lee Myers and Ellen Barry, "Putin Reclaims Crimea for Russia and Bitterly Denounces the West", *The New York Times*, 18 March 2014, https://www.nytimes.com/2014/03/19/world/europe/ukraine.html.

[48] Shaun Walker, "Putin admits Russian military presence in Ukraine for first time", *The Guardian*, 17 December 2015, https://www.theguardian.com/world/2015/dec/17/vladimir-putin-admits-russian-military-presence-ukraine.

[49] Mark Clayton, "Russia Hammers Ukraine with Massive Cyber-Attack", *Business Insider*, 15 March 2014, https://www.businessinsider.com/russia-cyberattack-ukraine-2014-3.

[50] Adrian Croft and Peter Apps, "NATO websites hit in cyber attack over Crimea stance", *Reuters*, 16 March 2014, https://www.reuters.com/article/us-ukraine-crisis-nato/nato-websites-hit-in-cyber-attack-over-crimea-stance-idUSBREA2F01R20140316/.

[51] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers", *The Christian Science Monitor*, 17 June 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

[52] Janne Hakala and Jazlyn Melnychuk, "Russia's Strategy in Cyberspace", NATO Strategic Communications Centre of Excellence, June 2021, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

[53] Anastasiia Lapatina, "The origins of the 2014 war in Donbas", *The Kyiv Independent*, 10 August 2023, https://kyivindependent.com/the-origins-of-the-2014-war-in-donbas/.

[54] Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry", *POLITICO*, 14 February 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

begin launching extensive cyberattacks against Ukraine. As a result, Ukraine's situation would end up being termed "Russia's test lab" for cyber war.[55]

In 2015, Russia conducted an unprecedented hack of Ukraine's power grid, which marked one of the first known instances of a cyberattack resulting in a major power outage, this one affecting around 230,000 residents of Western Ukraine.[56] The hackers used a spear phishing scheme with malicious Microsoft Office attachments to first gain access to the networks by obtaining the legitimate credentials of three regional electricity distribution companies, providing them with remote access. They sent malicious emails to employees, which, when opened, infected their operating systems.

The attackers deployed BlackEnergy malware on the companies' computer networks, which was used to gather intelligence on infrastructure and networks to guide future cyberattacks.[57] The hackers took over the control systems of the power distribution stations and manually switched off the electricity. The power was only out for one to six hours in the affected areas, but even two months after the attack, the control centres were still not fully operational.[58]

The attack was carefully planned and executed over many months with one of Russia's political goals being to undermine public trust in the Ukrainian Government and private companies. Viktor Yushchenko, who was Ukraine's president from 2005 to 2010, highlighted that Russia's tactics in the digital and physical realm are intended "to destabilize the situation in Ukraine, to make its government look incompetent and vulnerable".[59] Russia also began using these attacks against Ukraine to learn about the impact and to perfect its craft for future attacks against both Ukraine and the West.[60] The attack on Ukraine's critical infrastructure served as a wake-up call for the international community about the potential dangers of cyber warfare and the impact it could have on civilians.

In 2016, Russia conducted another cyberattack targeting Ukraine's critical infrastructure.[61] This attack specifically targeted the electrical grid of Kyiv, the capital of Ukraine, and marked a continuation of the cyber war tactics that were evident in the 2015 attack on Ukraine's power grid in Western Ukraine. The 2016 cyberattack used a more sophisticated approach by deploying a new type of malware known as "Industroyer". Industroyer is highly sophisticated and dangerous because it is designed to directly target and control electricity substation switches and circuit breakers.[62] This enables it to automate the process of controlling the electrical distribution network.

The blackout malware was similar to the Stuxnet attack as the aim was not only to disrupt physical infrastructure, but to destroy it.[63] The attack was also designed to cause prolonged

[55] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[56] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[57] Patrice Bock, "Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack", International Society of Automation (ISA), 23 September 2019, https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware.

[58] "Cyber-Attack against Ukrainian Critical Infrastructure", Cybersecurity and Infrastructure Security Agency, 20 July 2021, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[59] Greenberg, "How an Entire Nation".

[60] Alexander Salt and Maya Sobchuk, "Russian Cyber-Operations in Ukraine and the Implications for NATO", Canadian Global Affairs Institute, August 2021, https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato.

[61] Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction", *Wired*, 12 September 2019, https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

[62] Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", *We Live Security*, 12 June 2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[63] Greenberg, "New Clues Show".

harm, potentially resulting in power outages that could have lasted for weeks, if not months.[64] This showed that hackers were developing more sophisticated tools specifically designed to disrupt critical infrastructure, foreshadowing future Russian cyberattacks. Ukraine had become a "battleground in a cyberwar arms race for global influence".[65]

In what would become one of the most devasting cyberattacks ever launched, Ukraine was hit with an attack involving the NotPetya ransomware, which took place on 27 June 2017, Ukraine's Constitution Day.[66] This attack was particularly destructive and had a far-reaching impact, both on the country's infrastructure and also internationally as the cyberattack resulted in a global financial impact of US$10 billion worth of damage.[67] The primary objective of NotPetya was to disrupt Ukraine's financial system, but its effects extended well beyond that as it targeted a wide range of entities including banks, energy companies, government offices, airports and even some non-governmental organisations.[68] Within a span of 24 hours, NotPetya managed to erase data from 10% of computers across Ukraine, causing widespread disruption across various sectors.[69]

The malware initially spread through MeDoc, Ukraine's most popular accounting software.[70] Researchers discovered that some of MeDoc's software updates contained a hidden "backdoor".[71] This was likely implemented by someone with access to the company's source code and provided hackers with a stealthy way to infiltrate the systems of various companies without being detected. Unlike typical ransomware, which encrypts data and demands payment for its release, NotPetya was more destructive as it masqueraded as ransomware but was designed primarily to wipe data and disrupt systems. NotPetya also spread on its own and was a much more effective malware attack than in previous cases.[72]

However, former US Department of Homeland Security advisor Tom Bossert stated that the use of NotPetya was like "using a nuclear bomb to achieve a small tactical victory".[73] The attack also pointed out the interconnected nature of cyber vulnerabilities and how a cyberattack can rapidly spread around the globe from one piece of software. In essence, Ukraine's vulnerabilities in the cyber war against Russia are also the West's vulnerabilities. The need to help Ukraine shore up its defences was becoming more critical due to the fear of contagion in a globalised, interconnected world.

In July 2018, Russia attempted a cyberattack against a Ukrainian chlorine plant, the Auly Chlorine Distillation, with the intention of causing physical damage to the country's infrastructure.[74] The

[64] Greenberg, "New Clues Show".

[65] Cerulus, "How Ukraine became a test bed".

[66] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[67] Josephine Wolff, "How the NotPetya attack is reshaping cyber insurance", Brookings, 1 December 2021, https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

[68] Greenberg, "The Untold Story of NotPetya".

[69] Andrew E. Kramer, "Ukraine Cyberattack Was Meant to Paralyze, Not Profit, Evidence Shows", *The New York Times*, 28 June 2017, https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html.

[70] "Ukraine cyber-attack: Software firm MeDoc's servers seized", *BBC News*, 4 July 2017, https://www.bbc.com/news/technology-40497026.

[71] "Ukrainian Software Firm's Servers Seized after Cyber Attack", *NBCNews.com*, 4 July 2017, https://www.nbcnews.com/news/world/ukrainian-software-firm-s-servers-seized-after-cyber-attack-n779531.

[72] Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now", *CSO Online*, 17 October 2017, https://www.csoonline.com/article/563255/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

[73] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday, 2019), pp.17–18, pp.197–198.

[74] Catalin Cimpanu, "Ukraine Says It Stopped a VPNFilter Attack on a Chlorine Distillation Station", *BleepingComputer*, 12 July 2018, https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/.

facility is involved in the treatment of chlorine, which is vital for water purification and other industrial processes. The attackers used a malware known as "VPNFilter" which can survive a reboot, making it particularly resilient. The malware can be used for spying, stealing data, and disrupting industrial processes and can render devices inoperable.

The malware targeted the chlorine station's control systems, which could have interrupted how chlorine is treated and supplied. If the plant's operations were badly affected, it might have caused major environmental and health problems for the civilian population. This attack was planned to be Russia's next big cyberattack on Ukraine. However, before it could fully launch, security companies found the botnet, which had 500,000 infected devices. [75]

f) Russian Cyber Operations Against the West (2014–2022)

After gaining initial exposure to cyber operations against Ukraine and Georgia, Russia began expanding its targeting of Western states, especially after Putin first invaded Ukraine in 2014. Russia wanted to promote instability in Western democracies and to undermine the credibility of the democratic processes, according to former US ambassador to Russia Mike McFaul. [76] Following the illegal annexation of Crimea, Russia engaged in smaller-scale DDoS attacks to take out websites. However, it would grow bolder in its attacks against the West.

In 2015, German investigators found that hackers had successfully breached the computer network of the Bundestag, the German parliament. [77] This was considered the most significant cyberattack in German history due to the importance of the targeted institution, as Germany believed that Russia wanted to steal information to disrupt its democratic elections. In 2016, there was a cyberattack on the Christian Democratic Union (CDU), the political party then led by Chancellor Angela Merkel. [78] The attackers targeted the CDU to gain access to sensitive information. The primary objective was to acquire account names and passwords of party members, which would grant access to internal communications and potentially confidential data. However, the attack was not successful. But it continued to show Russia that it could wage cyber war against the West without fear of retribution.

Russia has been implicated in a series of cyberattacks against the UK, targeting various sectors. The UK has been one of Ukraine's strongest Western backers since Russia's first invasion in 2014.

One of the major cyber operations attributed to Russia was organised by the Federal Security Service (FSB). The UK Government has identified the FSB's Centre 18, and its unit Star Blizzard, as being responsible for sustained attempts to interfere in UK politics. This included spear phishing attacks on parliamentarians in a range of political parties from 2015 onwards, hacks of UK–US trade documents before the 2019 general election, and breaches of think tanks and civil society organisations. [79] The attacks aimed to undermine trust in UK politics and democratic processes and leak secret documents.

The United States has borne the brunt of major Russian cyberattacks since Russia invaded Ukraine. In 2014, Russian hackers launched an industrial sabotage campaign by targeting oil

[75] Cimpanu, "Ukraine Says It Stopped a VPNFilter Attack on a Chlorine Distillation Station".

[76] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Countries", *NBCNews.com*, 18 December 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

[77] Janosch Delcker, "Germany fears Russia stole information to disrupt election", *POLITICO*, 20 March 2017, https://www.politico.eu/article/hacked-information-bomb-under-germanys-election/.

[78] Jörg Blank, "Hacker-Attacke auf Merkels CDU-Zentrale", *bild.de*, 13 May 2016, https://www.bild.de/politik/inland/regierung/hacker-attacke-auf-cdu-zentrale-45802402.bild.html.

[79] "UK exposes attempted Russian cyber interference in politics and democratic processes". GOV.UK, 7 December 2023, https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes.

and gas companies in the West.[80] The most notorious incident occurred in 2016 when there was interference in the US presidential election with Russian hackers breaching the Democratic National Committee and leaking sensitive information to WikiLeaks.[81]

The global reach of Russian cyber operations was evident in 2017 with the NotPetya attack which initially targeted Ukraine but caused considerable collateral damage to the US and other Western companies.[82] The White House press secretary's office reported that the cyberattack was connected to the Russian goal of destabilising Ukraine.[83] Tariq Ahmad, UK Minister for Cybersecurity at the Foreign Office, described the attack as "reckless", emphasising its blatant disrespect for Ukrainian sovereignty. He highlighted the vast financial impact of the attack, noting that it cost European organisations hundreds of millions of pounds.[84] NotPetya showed that even though Ukraine is the epicentre for Russia's cyber aggression, the impact of this cyber war is global. Helping to defend Ukraine in cyberspace will defend all of the West.

In 2018, the US energy grid and other critical infrastructure sectors faced targeted attacks from Russian Government hackers, prompting a joint government alert between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).[85] The hackers also targeted vendors and smaller companies with weaker defences, using techniques like spear phishing as stepping stones to gain access to more significant networks and install malware.[86] Once inside, the hackers observed and learned how the computer systems worked, gaining greater insight into how power plants work and transmit data. Russia's goal from the hack was to showcase its growing cyber power and demonstrate its ability to hack critical infrastructure in the US.[87]

Without a strong response to deter future attacks, and despite hacking critical infrastructure in the West considered to be crossing red lines, Russia would only grow bolder with its cyberattacks. A sophisticated espionage campaign was discovered in 2020 with the SolarWinds hack, which allowed Russian hackers access to numerous companies and US Government agencies through compromised IT management software. The SolarWinds cyberattack remained unnoticed for several months while the company distributed software updates embedded with the hackers' code to its clients globally. This attack enabled hackers to gain access to various US Government networks, including those operated by the Department of Homeland Security and the Treasury Department.[88] The US Government followed up after the attack with sanctions against Russia.[89] Through a routine software update, Russia had

[80] Nicole Perlroth, "Russian Hackers Targeting Oil and Gas Companies", *The New York Times*, 30 June 2014, https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html.

[81] Ellen Nakashima and Shane Harris, "How the Russians hacked the DNC and passed its emails to WikiLeaks", *The Washington Post*, 13 July 2018, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

[82] Alfred Ng, "US: Russia's NotPetya the Most Destructive Cyberattack Ever", *CNET*, 15 February 2018, https://www.cnet.com/news/privacy/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine.

[83] Ibid.

[84] Ibid.

[85] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", Cybersecurity and Infrastructure Security Agency, 16 March 2018, https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical.

[86] Kelsey Atherton, "It's not just elections: Russia hacked the US electric grid", *Vox*, 28 March 2018, https://www.vox.com/world/2018/3/28/17170612/russia-hacking-us-power-grid-nuclear-plants.

[87] Bill Ibelle, "Russian cyberattack on US power grid meant to be show of power, researchers working to thwart the next one", *Northeastern Global News*, 21 March 2018, https://news.northeastern.edu/2018/03/21/northeastern-researchers-address-russian-power-grid-attack/.

[88] Scott Neuman and Dustin Jones, "U.S. Slaps New Sanctions On Russia Over Cyberattack, Election Meddling", *NPR*, 15 April 2021, https://www.npr.org/2021/04/15/987585796/u-s-slaps-new-sanctions-on-russia-over-cyber-attack-election-meddling.

[89] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack", *NPR*, 16 April 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

conducted “one of the most effective cyber-espionage campaigns of all time,” according to Alex Stamos, director of the Internet Observatory at Stanford University.[90]

US and European governments began grappling with the uncertainty regarding cyber red lines, and this intensified in the wake of the SolarWinds breach. In response to the attack, Marcus Willett, a former senior cyber advisor to Britain’s digital intelligence agency GCHQ, cautioned the US to be reserved in its response to Russia’s “surgical” espionage campaign.[91] Russian threat actors have long exploited the lack of clarity in cyber policy and have continued to leverage this ambiguity further.[92]

In May 2021, Colonial Pipeline was hit with a ransomware attack by a Russian criminal group that impacted the pipeline’s IT systems.[93] The attack was so devasting it led to jet fuel shortages for airlines and created long queues at petrol stations and a spike in petrol prices.[94] People were rushing to fill plastic bags with petrol, and the government had to issue a warning for people to only use containers intended for use with fuel, and several US states had to declare a state of emergency.[95]

Supply chain attacks, such as the Colonial Pipeline incident, often exploit vulnerabilities in a component within an organisation’s network. Tracking all application components and potential software vulnerabilities is challenging even for large organisations. In response, the Biden Administration issued an executive order to US agencies in May 2021 requiring them to enhance their cybersecurity, including adopting Software Bills of Materials (SBOMs).[96] SBOMs assist in identifying and updating software components, thus enabling quicker responses to vulnerabilities, and assisting buyers in assessing product risks.

A month later, JBS Foods, a major meat processing company, fell victim to a ransomware attack by a Russia-based group, forcing all nine of its beef plants to temporarily close.[97] The attack also affected its poultry and pork processing plants in the US. This shutdown had serious implications for the meat supply chain in the US, with concerns about potential shortages and spikes in meat prices. The White House placed the blame for the attack on Russia and said it was “considering all options regarding how to respond”.[98] However, Russia continued its pattern of bold cyberattacks which were never followed by a strong response from the West.

Cyber Warfare Following Russia’s Full-scale Invasion of Ukraine (2022 - Present)

Russia’s full-scale invasion of Ukraine in February 2022 marked the start of the world’s first cyber war due to the unprecedented scale and sophistication of the cyber operations that

[90] Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack”.

[91] Marcus Willett, “Lessons of the SolarWinds hack”, International Institute for Strategic Studies (IISS), 31 March 2021, https://www.iiss.org/online-analysis/survival-online//2021/04/lessons-of-the-solarwinds-hack.

[92] “Microsoft Digital Defense Report”, Microsoft, October 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

[93] Ken Dilanian and Kelly O’Donnell, “Russian criminal group suspected in Colonial pipeline ransomware attack”, *NBCNews.com*, 10 May 2021, https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793.

[94] Sean Michael Kerner, “Colonial Pipeline hack explained: Everything you need to know”, *TechTarget*, 26 April 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[95] “US states declare emergency over gas shortage fears”, *Deutsche Welle (DW)*, 12 May 2021, https://www.dw.com/en/us-states-declare-emergency-over-gas-shortage-fears-following-cyberattack/a-57501414.

[96] “What Is Executive Order 14028, Who Is Affected and How to Comply”, *Cybeats*, 23 March 2023, https://www.cybeats.com/blog/what-is-executive-order-14028-who-is-affected-and-how-to-comply.

[97] Julie Creswell, Nicole Perlroth and Noam Scheiber, “Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business”, *The New York Times*, 1 June 2021, https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.

[98] Catherine Thorbecke, Ben Gittleson and Luke Barr, “White House puts blame on Russia for JBS ransomware attack, weighs responses”, *ABC News*, 2 June 2021, https://abcnews.go.com/Business/white-house-contact-russia-meat-producer-jbs-hit/story?id=78021754.

accompanied Russia's military actions. It gave the world insight into how cyber operations would be integrated with the physical battlefield going forward. Moreover, Ukraine showcased to the international community not only the critical importance of robust cyber defences but also the complexity involved in their implementation. This complexity arises from the coalition that extends beyond the support of Western governments to include the pivotal contributions of tech companies in strengthening Ukraine's cyber defences.

In the months leading up to Russia's full-scale invasion of Ukraine in February 2022, a series of cyberattacks were launched against Ukrainian targets. On 13 January, Microsoft detected and reported malware targeting the Ukrainian Government, along with various non-profit organisations and IT companies.[99] This discovery was part of a broader pattern of digital aggression attributed to Russia.

The following day, Russia escalated its cyber war, conducting a significant cyberattack that affected various Ukrainian Government institutions and resulted in dozens of Government websites being controlled by hackers.[100] In response, NATO stepped up its support for Ukraine in the cyber domain, which included providing Ukraine with access to NATO's system for sharing information about malicious software.[101]

The cyberattacks continued into mid-February, culminating in a DDoS attack that temporarily disabled the online services of several Ukrainian Government departments, financial institutions and radio stations. The attacks took down Ukraine's two largest banks, PrivatBank and Oschadbank. PrivatBank had to release a statement assuring the public that there was no threat to depositors' funds.[102] These attacks were intended to create panic and confusion and to destabilise Ukraine and were attributed to Russia's Ministry of Defence Intelligence Directorate (GRU).[103]

On 24 February 2022, one hour before Russia began its full-scale invasion, a cyberattack with a wiper malware called AcidRain was launched on the American commercial satellite internet company Viasat, erasing all the data on its systems.[104] This attack caused outages not only for thousands of Ukrainian customers, but also impacted wind farms and internet users in other European countries. Russia's primary target was believed to be the Ukrainian military as it wanted to disrupt Ukrainian military communications at the onset of the Russian invasion, hindering Ukraine's defensive capabilities as Russia invaded the country. Ukraine's army relied on Viasat's services for maintaining command and control.[105] Russia had attempted to coordinate cyberattacks with its ground invasion to maximise its operations on the ground and to showcase the devastating damage that could be caused to critical infrastructure ahead of an invasion.

The most devastating attack on Ukraine's critical infrastructure came in December 2023 when Russia took down Kyivstar, Ukraine's biggest mobile network operator, damaging much of

[99] "Destructive malware targeting Ukrainian organizations", Microsoft, 15 January 2022, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[100] Jakub Przetacznik with Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks", European Parliament, June 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

[101] Pavel Polityuk and Steve Holland, "Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war", *Reuters*, 14 January 2022, https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/.

[102] "Ukraine's defence ministry and two banks targeted in cyberattack", *euronews*, 15 February 2022, https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack.

[103] "Attribution to Russia of malicious cyber activity against Ukraine", Australian Department of Foreign Affairs and Trade, 21 February 2022, https://www.internationalcybertech.gov.au/Attribution-to-Russia-of-malicious-cyber-activity-against-Ukraine.

[104] Patrick Howell O'Neill, "Russia hacked an American satellite company one hour before the Ukraine invasion", *MIT Technology Review*, 10 May 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

[105] Ibid.

the telecom company's IT infrastructure. [106] This could have been in retaliation for Ukrainian intelligence hacking Russia's state tax service (this attack happened right before the Kyivstar incident), which completely destroyed the agency's infrastructure and will impact the functioning of the agency for years to come. [107]

Over half of Ukraine's population uses Kyivstar and, as a result, millions were unable to receive lifesaving air raid alerts. Kyivstar CEO Oleksandr Komarov described the attack as "the biggest cyber attack on telco infrastructure in the world". [108] Komarov also pointed out that Kyivstar has repelled over 500 attacks on its infrastructure since the full-scale invasion started. [109] Around 30% of the cashless payment terminals of PrivatBank – Ukraine's largest bank – stopped working as they rely on Kyivstar's mobile network. [110] The hackers were able to breach Kyivstar via a compromised account belonging to an employee. [111] The Kyivstar incident underscores a key cybersecurity lesson: even the most fortified infrastructures are vulnerable to breaches, often due to the human factor, which can serve as the weakest link in security defences.

Illia Vitiuk, head of the Security Service of Ukraine's cybersecurity division, said that the hackers had been infiltrating Kyivstar since at least May 2023. He said that the attack should serve as a "big warning" to the West that no one is untouchable as Kyivstar had invested heavily in protecting itself. The cyberattack "completely destroyed the core of a telecoms operator". [112]

Following the Kyivstar attack by Russia, Ukraine retaliated with a cyberattack against Moscow-based water utility company Rosvodokanal, destroying the company's IT infrastructure. Over 50TB of data was deleted, "including internal document management, corporate email, backups, and even cybersecurity protections. [113] Ukrainian hackers allegedly affiliated with Ukraine's security services followed up by striking the Russian internet provider M9com on 9 January 2024; over 20 terabytes of data were deleted, and Moscow residents lost internet and TV connections. [114] The IT Army of Ukraine followed up with an attack on the Moscow-based internet provider, Qwerty, which was taken offline for over three days. [115]

Also, in January 2024, Ukraine's military intelligence agency conducted a cyberattack on IPL Consulting, a company which supports the Russian heavy industry and military-industrial complex, reportedly obliterating the firm's IT infrastructure. [116] After infiltrating and deleting

[106] Max Hunder, Jonathan Landay and Stefaniia Bern, "Ukraine's top mobile operator hit by biggest cyberattack of war", *Reuters*, 13 December 2023, https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/.

[107] Daryna Antoniuk, "Ukraine's intelligence claims cyberattack on Russia's state tax service", *The Record*, 12 December 2023, https://therecord.media/ukraine-intelligence-claims-attack-on-russia-tax-service.

[108] Olena Harmash, "Kyivstar Starts Restoring Voice Services – CEO", *Reuters*, 13 December 2023, https://www.reuters.com/technology/cybersecurity/kyivstar-starts-restoring-voice-services-ceo-2023-12-13/.

[109] "Ukraine's Main Phone Operator Recovering Two Days after Cyberattack", *Barron's*, 14 December 2023, https://www.barrons.com/news/ukraine-s-main-phone-operator-recovering-two-days-after-cyberattack-41ba9ee3.

[110] "Kyivstar network outage affects 30% of PrivatBank payment terminals", *Yahoo News*, 12 December 2023, https://news.yahoo.com/kyivstar-network-outage-affects-30-212000899.html.

[111] "Hackers breached Kyivstar's security through employee account – CEO", *Ukrainska Pravda*, 13 December 2023, https://www.pravda.com.ua/eng/news/2023/12/13/7432953/.

[112] Tom Balmforth, "Exclusive: Russian hackers were inside Ukraine telecoms giant for months", *Reuters*, 5 January 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

[113] Becky Bracken, "Russian Water Utility Hacked in Retaliation for Kyivstar Hit," *Dark Reading*, 21 December 2023, https://www.darkreading.com/ics-ot-security/ukrainian-hackers-strike-russian-water-utility.

[114] "Ukrainian hacking group claims retaliatory cyber-strike on major Moscow ISP", *Yahoo News*, 9 January 2024, https://news.yahoo.com/ukrainian-hacking-group-claims-retaliatory-122500493.html.

[115] Leo Chiu, "Moscow Internet System Reportedly Down for Three Days in Latest Ukrainian Cyberattack", *Kyiv Post*, 16 January 2024, https://www.kyivpost.com/post/26820.

[116] Martin Fornusek, "Military intelligence claims cyberattack on IT company providing services to Russian defense industry", *The Kyiv Independent*, 27 January 2024, https://kyivindependent.com/military-intelligence-claims-powerful-cyberattack-on-russian-it-company/.

over 60 terabytes of data from IPL Consulting's network, Ukrainian cyber experts destroyed numerous servers and databases, with the total cost of the damage still under assessment. The Russia–Ukraine cyber war is becoming more aggressive than ever and will continue to expand in the future to potentially more devastating critical infrastructure targets.

IV. How Ukraine Has Resisted Russia's Cyber Offensive

Paul Chichester, Director of Operations at the UK's National Cyber Security Centre (NCSC), describes the cyber war between Russia and Ukraine as "the most sustained set of cyber operations coming up against the best collective defence we have seen". [117] Ukraine's cyber defences have proven to be exceptionally robust, effectively preventing what could have been Russia's "cyber Pearl Harbor" – a devastating, surprise cyberattack intended to cause widespread disruption. Ukraine has effectively countered Russia's cyber threat by demonstrating a level of defensive strength and resilience that mirrors its tenacity on the battlefield. It has been reported that Russian hackers conducted at least 260 million attempts to break into Ukrainian systems between the start of the full-scale invasion and June 2023. [118]

Learning from past experiences, Ukraine has been able to develop a robust cyber defence to withstand Russia's onslaught. However, it is important to note that a critical factor in this success has been the extensive cyber support provided by Western governments. This support extends beyond mere diplomatic backing, encompassing technical and strategic assistance to bolster Ukraine's cyber capabilities. Equally important has been the role of technology companies. These entities have provided vital resources and expertise, contributing significantly to the strengthening of Ukraine's cyber defences. In March 2020, the Cyber Defense Assistance Collaborative for Ukraine (CDAC) was established to coordinate assistance from Western tech companies to support Ukraine. [119] The organisation helped to establish an "inventory of the potential services and products and tools foreign companies can offer to Ukraine and then also coordinate with different Ukrainian agencies and understand their needs as quickly as possible." [120]

In December 2021, a few months before Russia's full-scale invasion, the US military Cyber Command sent a team to Ukraine to analyse Ukrainian systems and whether Russian hackers had already penetrated them. [121] Their mission was to "hunt forward" and identify computer networks that had already been penetrated to help bolster Ukraine's defence amid heightened Russian aggression. As a result, Ukraine has fared better on the cyber front than many expected in the initial days of the war. Much of the cyber support provided by the West is done in secrecy and is likely to be far greater in scope than has been reported in the news.

Ukraine's Experience 2014–2022

Ukraine has had extensive experience fighting Russia on the cyber battlefield since 2014. As one Ukrainian official put it: "With their nonstop attacks, Russia has effectively been training us since 2014. So, by February 2022, we were ready and knew everything about their capabilities." [122] Russia's constant cyberattacks against the country have also increased societal awareness of cybersecurity and the role that civil society would need to play in cyber resilience. [123]

[117] Gordon Corera, "Ukraine war: Don't underestimate Russia cyber-threat, warns US", *BBC News*, 11 May 2022, https://www.bbc.com/news/technology-61416320.

[118] Maxim Tucker, "Still standing after 260m attacks: inside Ukraine's cyber warfare squad", *The Times*, 2 June 2023, https://www.thetimes.co.uk/article/still-standing-after-260m-attacks-inside-ukraines-cyber-warfare-squad-pxkqdp3pt.

[119] "Bilyana Lilly on Western cybersecurity assistance to Ukraine", *CyberScoop*, 5 September 2023, https://cyberscoop.com/bilyana-lilly-cybersecurity-assistance-ukraine/.

[120] Ibid.

[121] Gordon Corera, "Inside a US military cyber team's defence of Ukraine", *BBC News*, 30 October 2022, https://www.bbc.com/news/uk-63328398.

[122] Vera Mironova, "Russia's invasion of Ukraine is also being fought in cyberspace", Atlantic Council, 20 April 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/russias-invasion-of-ukraine-is-also-being-fought-in-cyberspace/.

[123] Khrystyna Kvartsiana, "Ukraine's Cyber Defense: Lessons in Resilience", German Marshall Fund of the United States, 22 November 2023, https://www.gmfus.org/news/ukraines-cyber-defense-lessons-resilience.

Russia also underestimated Ukraine's cyber abilities to resist. As Yurii Shchyhol, head of Ukraine's State Service of Special Communications and Information Protection, explained:

> "Ukraine's experience over the past year has underlined that cyberattacks require both time and knowledge to prepare. This helps explain why there have been fewer high-complexity cyber offensives following the initial failure of Russia's invasion strategy in spring 2022. Russia simply did not expect Ukraine to withstand the first big wave of cyberattacks and did not have sufficient plans in place for such an eventuality." [124]

The Role of the West's Private Sector

The private sector in the West has played an important role in helping keep Ukraine online. The involvement of Western private sector entities, primarily major technology and cybersecurity firms, has played a significant role in helping keep Ukraine online. These companies have provided expertise, resources, and sometimes direct assistance in securing Ukraine's digital infrastructure. Anti-DDoS assistance provided by companies like Cloudflare and Google was crucial for keeping much of Ukraine's infrastructure up and running against the onslaught of Russian DDoS attacks. [125]

Companies like Amazon and Microsoft helped move Ukrainian governmental operations and data into the cloud and, as a result, minimised the impact from both kinetic and cyber wiper attacks from Russia. Georgii Dubynski, the Deputy Minister for Digital Transformation of Ukraine, believes that Ukraine's partnerships with private entities in the West have played a crucial role in its cyber defence and resilience. [126]

Nick Beecroft from the Carnegie Endowment highlighted that:

> "A further defining feature of the defensive effort has been the integration of large American technology providers, particularly Amazon, Cloudflare, Google, and Microsoft. These companies' ability to migrate Ukrainian government data and services to distributed cloud servers; provide automated protection of massive networks, coupled with dedicated protection of high-risk users; as well as continually update threat intelligence drawn from global telemetry has added defensive depth and resilience far beyond that which Ukraine could have achieved independently." [127]

As a result, over 10 million gigabytes of Ukrainian Government and economic data was saved by taking it out of Ukraine and putting it into the cloud. [128] Ukraine's Deputy Prime Minister and Minister of Digital Transformation Mykhailo Fedorov even stated that "AWS [Amazon Web Services] made one of the biggest contributions to Ukraine's victory by providing the Ukrainian government with access and resources for migrating to the cloud and securing critical information." [129]

[124] Yurii Shchyhol, "Russia's cyberwar against Ukraine offers vital lessons for the West", Atlantic Council, 31 January 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/russias-cyberwar-against-ukraine-offers-vital-lessons-for-the-west/.

[125] "Bilyana Lilly on Western Cybersecurity Assistance to Ukraine".

[126] Jen Patja, Benjamin Wittes and Georgii Dubynski, "The Lawfare Podcast: Georgii Dubynskyi on Ukraine's Cybersecurity", The Lawfare Institute, 14 November 2022, https://www.lawfaremedia.org/article/lawfare-podcast-georgii-dubynskyi-ukraines-cybersecurity.

[127] Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense", Carnegie Endowment for International Peace, 3 November 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

[128] Katherine Tangalakis-Lippert, "Amazon helped rescue the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: 'You can't take out the cloud with a cruise missile'", *Business Insider*, 18 December 2022, https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12.

[129] "How Amazon is assisting in Ukraine", Amazon, 21 June 2023, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine.

Microsoft will continue to offer cloud services to Ukrainian Government institutions, including the military, schools, universities and hospitals, free of charge for another year across 2024, according to Fedorov.[130] This extension is part of the US$540 million in free services, technical support, equipment and grants provided by Microsoft to Ukraine. Beyond financial savings for the state budget, this support has been crucial in digitising Ukraine's government and protecting key government information from being destroyed or lost in Russian attacks.

As a result of being a strong supporter of Ukraine, providing extensive support for its cyber defence, Microsoft itself has been a target of Russian cyberattacks. Microsoft recently announced that the Russian state-sponsored hacker group Nobelium, known for the sophisticated SolarWinds attack, targeted its corporate systems. The company reported that Nobelium accessed the email accounts of some senior leadership team members late last year.[131]

Western Support for Ukraine's Cyber Defences

Western investment into Ukraine's cyber defences since 2014 has helped Ukraine withstand Russian attacks. Western countries have provided Ukraine with advanced technological tools and infrastructure to strengthen its cybersecurity. This has included sophisticated software for detecting and mitigating cyber threats, hardware to bolster network security, and platforms for enhanced monitoring and analysis of cyber activities, with companies like Microsoft providing threat intelligence data to Ukraine. A significant factor in Russia's failed cyber offensive was its underestimation of Ukraine's cyber defence capabilities. Western support and investments in Ukraine's cyber infrastructure since 2014 have significantly bolstered its defences. Russian cyberattacks didn't fail outright, rather, nearly 10 years of cyber war and significant Western investment, including public-private partnerships, have helped forge a strong defence.[132] Therefore, Ukraine's ability to quickly respond to and mitigate the effects of Russian cyberattacks has diminished the impact these attacks might have had.

David Luber, Deputy Cybersecurity Director at the US National Security Agency (NSA), in commenting on the strategy of defending forward, highlighted that:

> "as United States Cyber Command deployed their troops to train [Ukrainians] prior to the invasion, we worked very closely with them as they looked at that defense. And as they found malicious software and malicious activity, we worked with them to [ensure] that information is shared broadly with both government and industry, not only to protect Ukraine, but also to protect NATO, to protect other allies and the US."[133]

Protecting Ukraine's networks also protects Western networks.

Since 2014, the United States has significantly contributed to enhancing Ukraine's energy security, providing over US$160 million in technical assistance.[134] This collaboration involved the US Department of Energy working closely with the Ukrainian Government to fortify the resilience of Ukraine's energy infrastructure and improve national response strategies, particularly in the wake of cyberattacks targeting the country's electric grid.[135] These efforts

[130] Nate Ostiller, "Minister: Microsoft to provide free cloud services to Ukrainian government for another year", *The Kyiv Independent*, 29 November 2023, https://kyivindependent.com/minister-microsoft-to-provide-free-cloud-services-to-ukrainian-government-for-another-year/.

[131] Tom Warren, "Microsoft 'senior leadership' emails accessed by Russian SolarWinds hackers", *The Verge*, 19 January 2024, https://www.theverge.com/2024/1/19/24044561/microsoft-senior-leadership-emails-hack-russian-security-attack.

[132] Sydney J. Freedberg Jr, "'No Big Bang': Cyber successes in Ukraine are no cause for complacency in US", *Breaking Defense*, 20 January 2023, https://breakingdefense.com/2023/01/no-big-bang-cyber-successes-in-ukraine-are-no-cause-for-complacency-in-us/.

[133] Ibid.

[134] "Energy Security Support to Ukraine", U.S. Department of State, 29 November 2022, https://www.state.gov/energy-security-support-to-ukraine/.

[135] "U.S.-Ukraine Energy Cooperation", Department of Energy, https://www.energy.gov/ia/us-ukraine-energy-cooperation.

led to a marked reduction in the effectiveness of Russian cyberattacks, which had previously caused considerable damage following Russia's initial invasion of Ukraine in 2014.[136] By 2022, thanks to these strengthened defences, Ukraine's energy infrastructure remained robust against these cyber threats. As a result, Russia resorted to the use of cruise missiles and drones in an attempt to disrupt and destroy Ukraine's power grid.[137]

Russia's Failure to Integrate Cyber and Conventional Attacks

Russia has failed to successfully integrate cyber and conventional attacks on the battlefield. One of the primary issues was the apparent lack of synchronisation between Russia's cyber operations and its ground forces. Effective integration requires that cyberattacks be timed and targeted to complement and enhance the effectiveness of physical military actions. But while Moscow aimed to utilise cyberattacks to gather intelligence in Ukraine, "Russian brutality and incompetence" reduced their ability to take advantage of the intelligence.[138] Russia's inadequate preparations to create coordinated strikes on critical targets provides lessons on what not to do in cyber war. Cyberattacks are most effective "when combined with other weapons, including conventional delivery systems, precision-guided munitions, unmanned aerial vehicles, and electronic warfare. This combination can cripple command networks and advanced weapons systems and contribute to the attrition of opposing forces."[139]

The Robust Cyber Defence Ecosystem

With Western support, defence has proven to be king in the cyber war between Russia and Ukraine. Russia's cyber war against Ukraine has faced a robust global response, with countries and international organisations providing extensive cybersecurity assistance to Ukraine which has helped the country thwart Russia's offensive. Microsoft President Brad Smith believes that the Russia-Ukraine cyber war has showed that "a new form of collective defense" has "proven stronger than offensive cyber capabilities."[140] Ukraine's cyber defence has relied on a coalition of partners supporting its defence, including governments, private companies and NGOs, versus Russia as a major cyber power.[141]

Private companies predominantly own and manage the world's computer code, equipment and network infrastructure, and they invest heavily in network surveillance to ensure they are kept running. Simultaneously, a blend of academic institutions, governments and non-profit organisations diligently seek out software bugs, providing regular updates to these companies about any shortcomings or vulnerabilities they discover.[142] As a result, there are robust ecosystems in place to assist with cyber defence, even more so in Ukraine's case, where Western governments and private companies have bolstered its defence. Developing a sophisticated cyber weapon can take years, but it can take seconds to delete the code that hosts the vulnerability.

[136] James Hesson and Annie Fixler, "Ukraine's Cyber Defense Offers Lessons for Taiwan", *Defense One*, 16 March 2023, https://www.defenseone.com/ideas/2023/03/ukraines-cyber-defense-offers-lessons-taiwan/384083/.

[137] Olena Harmash and Tom Balmforth, "Russia hits Ukrainian energy facilities in biggest attack in weeks, Kyiv says", *Reuters*, 21 September 2023, https://www.reuters.com/world/europe/blasts-heard-kyiv-other-parts-ukraine-2023-09-21/.

[138] Jon Bateman, Nick Beecroft and Gavin Wilde, "What the Russian Invasion Reveals about the Future of Cyber Warfare", Carnegie Endowment for International Peace, 19 December 2022, https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

[139] James Andrew Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies, 16 June 2022, https://www.csis.org/analysis/cyber-war-and-ukraine.

[140] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War", Microsoft, 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[141] Ibid.

[142] Grace B. Mueller, et al., "Cyber Operations during the Russo-Ukrainian War", Center for Strategic and International Studies, 13 July 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

V. Conclusion: Lessons for the UK from Ukraine’s Cyber War

It is important for the UK to recognise the rapidly changing nature of warfare and how agile non-state actors like hacktivist groups and their use of technology are being used by adversaries like Russia to advance their state interests. States like Russia are only increasing their cyber strength and the sophistication of their cyber threats. Carl von Clausewitz understood that only great strength of will can lead to the desired outcome.[143] Clausewitz emphasised the importance of willpower in achieving victory, both on the part of military leaders and their forces. He understood that war is not only a physical struggle but also a moral one, where the determination and resolve of the combatants can be as critical as their material resources. If the UK is genuinely committed to supporting Ukraine's victory on the battlefield, it must broaden its consideration of the resources it provides. This support should encompass not only conventional weaponry for physical combat but also include advanced cyber capabilities to bolster Ukraine's defence and offensive strategies in the digital realm.

Furthermore, Carl von Clausewitz’s assertion that “war is the continuation of politics by other means” is profoundly relevant in the context of modern cyber war. Russia views cyber war as an extension of its overall campaign to subjugate the Ukrainian people and destroy the state. Cyber war transfers political confrontations into the digital sphere, where the significance of physical borders and conventional military strength diminishes. In this realm, Clausewitz’s concept of the “fog of war” – emphasising the inherent uncertainty and chaos in warfare – becomes especially pertinent. Cyber war is characterised by its anonymity and the difficulty in attributing attacks, mirroring this “fog”.

The war in Ukraine exemplifies this. As Russia’s physical military engagement in Ukraine encountered setbacks, Moscow increasingly resorted to cyberattacks.[144] Russia’s intelligence services also create greater confusion by “falsely assuming the identities of anonymous political and hacktivist groups to misdirect attribution and generate second-order psychological effects from their cyber operations.”[145] These attacks, aimed at instilling terror among the Ukrainian populace, target critical services such as electricity and the internet. Rob Joyce, Cybersecurity Director at the NSA, observed that the prolonged nature of this conflict only increases Ukraine’s vulnerability to these destructive cyberattacks, particularly against its critical infrastructure.[146]

In looking to the future of the Russo–Ukrainian war, the intensity and scale of cyberattacks will continue to grow, as evidenced by recent attacks like the one on Kyivstar. Ukraine needs additional support for its cyber defences, much like it needs air defence systems to keep its physical cities safe. It is time to rethink how the West applies military doctrine in supporting Ukraine and to begin searching for new ways to support Ukraine’s cyber and physical battlefield offensives to defeat Russia and protect the Western world from further Russian aggression.

Lesson 1: Supporting Ukraine Increases the Risk of Cyberattacks on the UK

The more support the UK provides to Ukraine, the more cyberattacks Russia will conduct against the country. In January 2024, the UK signed an unprecedented security agreement

[143] Jared Ware, “Is Clausewitz Compatible with Cyber?”, *The Cyber Defense Review*, 11 August 2015, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136156/is-clausewitz-compatible-with-cyber/.

[144] Maggie Miller, “Russia’s cyberattacks aim to ‘terrorize’ Ukrainians”, *POLITICO*, 11 January 2023, https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

[145] Dan Black and Gabby Roncone, “The GRU’s Disruptive Playbook”, *Mandiant*, 12 July 2023, https://www.mandiant.com/resources/blog/gru-disruptive-playbook.

[146] Miller, “Russia’s cyberattacks aim to ‘terrorize’ Ukrainians”.

with Ukraine and provided a £2.5 billion military aid package.[147] As a result of being one of the biggest donors of military aid to Ukraine, the UK has also become the "third most targeted country in the world for cyber-attacks, after the US and Ukraine".[148] When NATO declared support for Ukraine in 2014 over Russia's initial invasion, Russia responded with DDoS attacks on NATO websites. Russian cyberattacks on the UK can be seen as a direct response to its support for Ukraine.

These attacks serve multiple purposes for Russia. Firstly, they act as a form of retaliation, aiming to penalise the UK for its support of Ukraine. Secondly, these attacks serve as a warning, signalling the consequences to other nations that might consider providing similar support to Ukraine. Finally, by targeting a key ally of Ukraine, Russia attempts to undermine the collective response and solidarity among Ukraine's supporters, and to seek to deter future aid. Britain's National Cyber Security Centre (NCSC) also warned in April 2023 of an increased risk to Western critical national infrastructure by Russian hackers.[149]

As the war grinds more and more into a stalemate, attacks on critical infrastructure in the UK are bound to start happening more frequently as Russia explores new attack vectors to target Ukraine's allies. Russian cybercriminals, with support from the state, have already been attacking the UK's critical infrastructure with ransomware attacks, and it is expected that these attacks will increase in the future.[150] Microsoft believes that as the war in Ukraine has become static and evolved into trench warfare, Russian cyberattacks will focus on degrading "Kyiv's external sources of military and financial assistance".[151]

The British Library was a recent target of a ransomware attack by Rhysida, a ransomware group believed to be from Russia.[152] The cyberattack brought down the library's catalogue and computer systems; it will take up to a year to repair the damage, draining around 40% of the library's reserves.[153] Rhysida also conducted an attack against London's King Edward VII Hospital, attempting to steal medical information from the British royal family.[154]

Lesson 2: Space Warfare Threats May Increase as Cyber is Countered

The failure of cyber operations to wield significant influence on the battlefield could lead to countries like China and Russia moving to be more aggressive in space warfare as another theatre. Ukraine's use of satellite networks has played a crucial role in sustaining military operations and being able to maintain communications across the country.[155] Afterall, this

[147] Zoya Sheftalovich, Veronika Melkozerova and Bethany Dawson, "Rishi Sunak hugs Ukraine close with security deal and extra cash", *POLITICO*, 12 January 2024, https://www.politico.eu/article/rishi-sunak-arrives-in-kyiv-with-2-5b-and-a-security-deal/.

[148] "How resilient is UK Critical National Infrastructure to cyber-attack?", UK Parliament, 24 October 2023, https://committees.parliament.uk/committee/135/science-innovation-and-technology-committee/news/198084/how-resilient-is-uk-critical-national-infrastructure-to-cyberattack/.

[149] James Pearson, "Russian hackers targeting Western critical infrastructure, UK says", *Reuters*, 19 April 2023, https://www.reuters.com/world/europe/russian-hackers-targeting-western-critical-infrastructure-uk-says-2023-04-18/.

[150] Rob Hastings, "Why Russia's cyberwarfare has failed in Ukraine – but remains a threat to the UK", *inews UK*, 13 June 2023, https://inews.co.uk/news/technology/russia-cyber-warfare-failed-ukraine-threat-uk-2404924.

[151] Clint Watts, "Russian influence and cyber operations adapt for long haul and exploit war fatigue", Microsoft, 7 December 2023, https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/.

[152] Dan Milmo, "Rhysida, the new ransomware gang behind British Library cyber-attack", *The Guardian*, 24 November 2023, https://www.theguardian.com/technology/2023/nov/24/rhysida-the-new-ransomware-gang-behind-british-library-cyber-attack.

[153] Robbie Griffiths, "'Totally and utterly bereft' – the devastating repercussions of the British Library cyber attack", *The Standard*, 12 January 2024, https://www.standard.co.uk/lifestyle/british-library-cyber-hack-rhysida-ransomware-tom-holland-b1131623.html.

[154] "Rhysida Ransomware Targeted Royal Family's Medical Records", *ITonDemand*, 14 December 2023, https://www.itondemand.com/2023/12/14/rhysida-ransomware-targeted-royal-familys-medical-records/.

[155] Christopher Miller, Mark Scott and Bryan Bender, "UkraineX: How Elon Musk's space satellites changed the war on the ground", *POLITICO*, 8 June 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

is why Russia attempted to take down Viasat at the start of the full-scale invasion. However, although Russia did manage to knock out Viasat services, Ukraine was able to restore them rather quickly. Russia has also attempted to attack SpaceX's Starlink services inside Ukraine.[156] Starlink, utilising modern DevSecOps tools akin to its parent company, SpaceX, provides Ukraine with rapid agility and enhanced security.[157] This approach enables swift execution of tasks that would traditionally take months for older satellite operators, which in Starlink's case, allows its infrastructure to be updated several times a day, reducing the risk of unpatched vulnerabilities. This is why Starlink has not been taken down. Instead of relying on cyberattacks to try and neutralise satellites in space, countries will likely opt to physically destroy them. While Viasat has a few satellites that cover large areas, Starlink has thousands of them in space, making them much more difficult to destroy. A combination of cyberattacks and missile strikes could be used to destroy communication systems.

Lesson 3: Actors are Increasingly Decentralised and Crowdsourced

Cyber warfare is being crowdsourced and decentralised. Hacking is quickly becoming a core part of military operations, and the role of non-state actors will only continue to grow.[158] In the period leading up to Russia's invasion of Ukraine, there was a significant surge in cyberattacks originating from Russia. The cybersecurity firm Kaspersky reported a 450% increase in such attacks year-on-year.[159] This escalation continued after the invasion, with a dramatic rise in DDoS attacks against United States national security targets. Many of these attacks have been linked to Killnet, a hacktivist group aligned with Russia, according to an investigation by NetScout.[160]

Another prominent group in this cyber offensive is NoName057(16), known for its manifesto that criticises the West for "Russophobia". Unlike traditional cyberattack strategies, NoName057(16) takes a unique approach by incentivising independent hackers to conduct DDoS attacks. It offers substantial rewards in cryptocurrency for successful attacks, essentially outsourcing its cyber warfare. The group has streamlined its recruitment and operation processes through an automated system on the messaging service Telegram.[161]

Since its inception in early 2022, NoName057(16) has rapidly expanded its reach, garnering over 52,000 subscribers by September 2023.[162] The group's cyberattacks have had a wide impact, disrupting the financial sector in Denmark, port operations in Dutch cities like Amsterdam and Groningen, and a range of businesses in Poland and Lithuania.[163] Similar attacks were conducted against the Icelandic parliament and the Council of Ministers, whose websites brought down by DDoS attacks from NoName057(16).[164]

[156] Mike Stone and Joey Roulette, "SpaceX's Starlink wins Pentagon contract for satellite services to Ukraine", *Reuters*, 1 June 2023, https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/.

[157] Vilius Petkauskas, "Why can't Russians hack Starlink satellites?", *Cybernews*, 15 November 2023, https://cybernews.com/security/why-cant-russians-hack-starlink-satellites/.

[158] Janosch Delcker, "Ukraine war: What's the impact of cyber guerrillas?", *Deutsche Welle (DW)*, 23 December 2023, https://www.dw.com/en/ukraine-war-whats-the-impact-of-cyber-guerrillas/a-67775539.

[159] Alexander Gutnikov, Oleg Kupreev and Yaroslav Shmelev, "DDoS Attacks in Q1 2022", *Securelist*, 25 April 2022, https://securelist.com/ddos-attacks-in-q1-2022/106358/.

[160] "DDoS Threat Intelligence Report", *NETSCOUT*, 2023, https://www.netscout.com/threatreport/ddos-threat-intelligence-report/.

[161] David Kirichenko, "Crowdsourced Cyber Warfare: Russia and Ukraine Launch Fresh DDoS Offensives", *CEPA*, 13 July 2023, https://cepa.org/article/russia-ukraine-launch-cyber-offensives/.

[162] Daryna Antoniuk, "What's in a NoName? Researchers see a lone-wolf DDoS group", *The Record*, 4 September 2023, https://therecord.media/noname-hacking-group-targets-ukraine-and-allies.

[163] Benedikt Stöckl, "Dutch ports fall victim to Russia-friendly hackers again", *Euractiv*, 21 June 2023, https://www.euractiv.com/section/politics/news/dutch-ports-fall-victim-to-russia-friendly-hackers-again/.

[164] Charles Szumski, "Cyberattacks target Icelandic official websites, tech companies", *Euractiv*, 14 June 2023, https://www.euractiv.com/section/politics/news/cyberattacks-target-icelandic-official-websites-tech-companies/.

While there is no direct evidence to suggest that Russian President Vladimir Putin controls NoName057(16), the group has demonstrated consistent support for him and Russian geopolitical goals. A notable deviation in its usual attack pattern occurred on 24 June 2023 when NoName057(16) focused its efforts on just two websites associated with Russian Wagner mercenaries. [165] This shift coincided with a bold but unsuccessful mutiny by Wagner mercenaries, suggesting a connection between NoName057(16) and Russian state activities. It also reflects the trend that while there may be civilians or hacktivists waging cyberattacks, their general direction is usually influenced by the desires of the government, both for Ukraine and Russia.

The Ukrainian side has been even more successful in crowdsourcing its cyber war. In response to Russia's full-scale invasion in February 2022, Ukraine quickly mobilised to form a volunteer IT army. This cyber militia, composed of hackers, grew rapidly, attracting tens of thousands of volunteers from across the globe. The IT Army of Ukraine has evolved from an initially ad-hoc assembly of volunteer cyber enthusiasts into a highly structured and efficient operation. This transformation is attributed to several factors. Firstly, ongoing support from Ukrainian Government officials, who likely provided strategic direction and legitimacy to their operations. Secondly, the involvement of international participants brought in a global perspective and a wealth of diverse cyber expertise. Finally, using industry-leading tools and technologies has greatly enhanced its operational effectiveness.

Ukraine's IT Army has made tangible impacts on the cyber war front. In February 2022, the group successfully orchestrated the takedown of high-profile Russian websites, including those of the Moscow Stock Exchange and Sberbank, Russia's largest bank. [166] This was a significant blow, disrupting the Kremlin's financial and economic activities. In October 2022, the IT Army's operations escalated to a more critical infrastructure level when it gained access to Loesk, an electrical utility company in the Leningrad region. [167] The intrusion led to power outages across the region, demonstrating the group's capability to impact essential services in Russia.

In November 2022, the IT Army targeted Gazprombank, the bank linked to Russia's state-owned energy company, Gazprom. The group stole 2.6GB worth of data, including 27,000 files containing information on the bank's operations and security policies and personal data of employees. The sophistication of this attack was even praised by Gazprombank vice president Olexander Egorkin for the creativity of the hackers. [168]

Ukraine's IT Army used a targeted DDoS attack to strike Russia's sole product authentication system (Chestny Znak). This system, critical for the verification and labelling of a wide range of products in Russia, serves an important function in the country's economic infrastructure. [169] The impact of this cyberattack was far-reaching and multifaceted. It forced the Russian Government to temporarily suspend the mandatory labelling and verification processes for certain products. This suspension had immediate and tangible consequences for Russian businesses, especially those in sectors heavily reliant on the verification system for their

[165] Amaury G and Charles M, "Following NoName057(16) DDoSia Project's Targets", *Sekoia.io Blog*, 29 June 2023, https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/.

[166] Sarah Coble, "Moscow Exchange Downed by Cyber-Attack", *Infosecurity Magazine*, 28 February 2022, https://www.infosecurity-magazine.com/news/moscow-exchange-cyber-attack/.

[167] "Ukrainian hackers switched off electricity for Leningrad region in Russia", *Technology Org*, 16 October 2022, https://www.technology.org/2022/10/16/ukrainian-hackers-switched-off-electricity-for-leningrad-region-in-russia/.

[168] Daryna Antoniuk, "Ukrainian hacktivists claim to leak trove of documents from Russia's central bank", *The Record*, 7 November 2022, https://therecord.media/ukrainian-hacktivists-claim-to-leak-trove-of-documents-from-russias-central-bank.

[169] "Russia, once considered a top force in cyberspace, now being mocked by world's best hackers", *Yahoo News*, 9 May 2022, https://news.yahoo.com/russia-once-considered-top-force-134600985.html.

daily operations. The inability to authenticate products led to a cascade of issues, including delays in the distribution of goods, challenges in maintaining inventory controls, and a general disruption in the market dynamics.

In October 2023, the Ukrainian IT Army was able to temporarily disable internet services in Russian-occupied south-eastern Ukraine. The IT Army's DDoS attacks knocked out three Russian internet providers – Miranda-media, Krimtelekom and MirTelekom. [170] In its most recent cyber offensive, in December 2023, Ukraine's IT Army successfully targeted and disrupted the servers of Bitrix24, a widely used customer relationship management (CRM) system in Russia. [171] This attack was part of an ongoing series of DDoS offensives against key Russian digital infrastructure. In December 2023, the IT Army, leveraging their official Telegram channel, declared that the successful disruption of Bitrix24 could potentially lead to substantial economic losses for Russia. The IT Army posted: "this could mean tens or even hundreds of millions of dollars in losses for the enemy's economy, depending on how long we can hold them down. Who else has idle devices? It's time to turn them on." The IT Army of Ukraine estimates its operations have produced economic damage to Russia amounting to one to two billion dollars. [172]

However, the two largest hacktivist groups in the Russo–Ukrainian war have both pledged to scale back cyberattacks and adhere to new engagement rules set by the International Committee of the Red Cross. [173] These rules, forming a "Geneva Code of cyber-war", aim to regulate civilian hacker activities, a move initially met with scepticism but now gaining traction among Ukrainian and Russian hackers. Despite the widespread impact of their previous attacks on civilian services in both countries, these groups, including the notorious pro-Russian Killnet, have committed to avoiding targets that affect civilians. Similarly, the IT Army of Ukraine, Ukraine's biggest civilian cyber group, has agreed to follow these guidelines as well.

Following one of the latest attacks by the IT Army, in January 2024, on the Russian energy provider Permenenergo, the group stated on its Telegram account that "per Red Cross cyber warfare rules", the electric supply for civilians in the Perm region was not disrupted. [174] The fallout from the Ukrainian cyberattack was that it "requires state funds for recovery and causes temporary loss of energy network control". [175] The IT Army also conducted multiple attacks against Moscow's primary internet provider, Akado Telecom, which caused widespread internet disruptions across Moscow's Government and banking sectors; among the affected were the presidential security unit, the FSO and Russia's intel agency, the FSB. [176]

Lesson 4: Critical Infrastructure is a Prime Target

Critical infrastructure will continue to be a prime target, even more so if the war in Ukraine continues to be at a stalemate. In May 2022, following the arrest of one of its associates, the cyber hacktivist group Killnet issued a threat that it would target critical medical equipment

[170] Daryna Antoniuk, "Ukrainian hackers disrupt internet providers in Russia-occupied territories", *The Record*, 28 October 2023, https://therecord.media/ukranian-hackers-disrupt-internet-providers-crimea.

[171] Daryna Antoniuk, "Ukrainian hacktivists claim attack on popular Russian CRM provider", *The Record*, 21 December 2023, https://therecord.media/bitrix24-disruption-ukraine-it-army.

[172] David Kirichenko, "How Ukraine built a volunteer hacker army from scratch", *Euromaidan Press*, 16 January 2024, https://euromaidanpress.com/2024/01/16/how-ukraine-built-a-volunteer-hacker-army-from-scratch.

[173] Joe Tidy, "Ukraine cyber-conflict: Hacking gangs vow to de-escalate", *BBC News*, 6 October 2023, https://www.bbc.com/news/technology-67029296.

[174] IT Army of Ukraine, "IT army blocks Permenenergo payments", *Telegram*, 13 January 2024, https://t.me/itarmyofukraine2022/1933.

[175] Ibid.

[176] Stefanie Schappert, "Putin's intel agencies lose internet, Ukraine IT Army takes claim", *Cybernews*, 24 January 2024, https://cybernews.com/cyber-war/russia-fsb-akado-internet-down-ukraine-it-army/.

in the UK, specifically lifesaving ventilators in British hospitals.[177] A cyberattack that interferes with these systems could lead to delayed or incorrect dispensing of essential drugs, posing serious risks to patient health. The potential impact of such cyberattacks extends beyond individual patient outcomes. A large and coordinated wave of cyberattacks against these life-critical systems in hospitals could lead to a broader healthcare crisis, putting numerous lives at risk, overwhelming the healthcare infrastructure, and potentially leading to people dying.[178]

UK Cabinet Office secretary Oliver Dowden issued a warning in April 2023 that Russian hackers seek to destroy Britain's infrastructure or, at the very least, disrupt operations.[179] The NCSC also warned of long-term threats to the UK's critical infrastructure.[180] While the US and Ukraine have suffered far more serious attacks on critical infrastructure, the UK could be vulnerable to an attack that paralyses the country and damages some of its critical infrastructure. The Joint Committee on the National Security Strategy believes that the UK could be brought to a halt "at any moment" by a cyberattack due to its critical infrastructure being vulnerable to ransomware.[181] In fact, the UK's most hazardous nuclear site has already been hacked into by groups linked to China and Russia.[182]

Lesson 5: Industrial Espionage by Russia Will Continue to Grow

Industrial espionage will continue to grow due to Western companies fleeing Russia and the impact of sanctions. Ukraine has seen an uptick in Russian cyber-espionage activity that has been attempting to penetrate the systems of important government agencies.[183] Natalia Tkachuk, head of Ukraine's Information Security and Cybersecurity Service, stated that:

> "The main thing to expect is the increasing use of criminal hacker groups by russian intelligence services to carry out intelligence and subversive activities against Western countries and targeted cyber operations. The new vector of such attacks will be industrial espionage. After all, as a result of the effective actions of sanctions, Russia has lost access to a significant number of leading technologies, which it cannot replace with their own, so they will try to steal them."[184]

Deprived of Western technologies, Russia will be compelled to rely on alternative solutions, which are likely to be less secure and more susceptible to Western cyberattacks. As Russia faces this technological gap, it may increasingly turn to industrial espionage in an attempt to acquire Western technology. Moreover, if Russia maintains significant access to Western technologies, the West may exhibit caution in deploying zero-day exploits against Russian targets, fearing collateral damage that could also impact Western entities.

[177] "Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector", U.S. Department of Health and Human Services, 30 January 2023, https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf.

[178] William Ralston, "The untold story of a cyberattack, a hospital and a dying woman", *Wired*, 11 November 2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany.

[179] Dan Sabbagh, "Russian hackers want to 'disrupt or destroy' UK infrastructure, minister warns", *The Guardian*, 19 April 2023, https://www.theguardian.com/technology/2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns.

[180] "NCSC warns of enduring and significant threat to UK's critical infrastructure", NCSC, 14 November 2023, https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure.

[181] "UK could be brought to a halt 'at any moment' by cyberattack, report warns", *Sky News*, 13 December 2023, https://news.sky.com/story/the-uk-could-be-brought-to-a-halt-at-any-moment-by-cyberattack-report-warns-13029226.

[182] Anna Isaac and Alex Lawson, "Sellafield nuclear site hacked by groups linked to Russia and China", *The Guardian*, 4 December 2023, https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups russia-china.

[183] Adam Janofsky, "From the front lines of 'the first real cyberwar'", *The Record*, 19 April 2022, https://therecord.media/from-the-front-lines-of-the-first-real-cyberwar.

[184] Ibid.

Lesson 6: Everything and Everyone is a Target

Everything and everyone can be a target for hacking. After Russia's full-scale invasion of Ukraine, a new kind of cyber war began to take shape involving information operations.[185] This cleverly involved using social media and dating apps. Russian soldiers, looking for friendship on Tinder, unknowingly gave away important military information.[186] They talked to fake profiles that resembled real Ukrainian women created using AI technology.[187] These chats led to the soldiers sharing pictures that revelated their location. This approach was also used by a Ukrainian woman who set up two Tinder accounts with different locations near the border.[188] By comparing where her matches were, she was able to figure out exactly where the Russian troops were located. She found and reported over 70 such profiles to Ukrainian officials, helping them gather valuable information.

The use of fake social media profiles didn't stop there. Ukrainian hackers made fake profiles of beautiful women on various platforms, like Telegram, to attract Russian soldiers near Melitopol.[189] According to the *Financial Times*, these tricked soldiers sent pictures showing them while on duty. The hackers then used the pictures to find out where a hidden Russian military base was located near Melitopol in southern Ukraine.[190] This important information was passed to the Ukrainian military which launched an attack on the base soon after.

However, soldiers are not the only victims of hacks and social engineering. Russian pensioners were targeted by phone call scammers who tricked them into firebombing military enlistment offices. A Russian security official stated that "the scammers had often persuaded their victims to hand over banking details, or take out a loan, before convincing them to attack a recruitment office in order to recoup their losses."[191] What this means for the future is that many individuals could be victims of a cyberattack that might steal their personal information or bank account details while enticing them to commit a crime or spy for a foreign government. A future resembling an episode of the science-fiction TV show *Black Mirror* may not be far off, where foreign governments, such as Russia, may hack the personal devices of random citizens and blackmail them into spying on UK bases.[192]

Russia also hacked online surveillance cameras in Kyiv to spy on air defence forces and critical infrastructure.[193] Originally installed on residential buildings for residents to monitor their surroundings, these cameras were reportedly commandeered by Russian intelligence. They gained remote access, altered the cameras' angles, and streamed sensitive footage on *YouTube*.

[185] David Kirichenko, "The Growing Use of Scamming Techniques and Social Media on the Battlefield", Irregular Warfare Center, 30 October 2023, https://irregularwarfarecenter.org/publications/perspectives/the-growing-use-of-scamming-techniques-and-social-media-on-the-battlefield/.

[186] Jesse O'Neill, "'Sleeping with the Enemy' Russian troops try to pick up Ukrainian women on Tinder", *New York Post*, 24 February 2022, https://nypost.com/2022/02/24/ukrainian-women-say-russian-troops-are-flirting-with-them-on-tinder/.

[187] Sophia Ankel, "Ukrainian women are using dating profiles with AI images to trick horny Russian soldiers into giving away secrets, report says", *Business Insider*, 20 July 2023, https://www.businessinsider.com/ukrainian-women-use-dating-profiles-get-intel-from-russian-soldiers-2023-7.

[188] Severija Bielskyte, "How Tinder became a weapon in the Russia-Ukraine War", *Huck Mag*, 21 March 2022, https://www.huckmag.com/article/how-tinder-became-a-weapon-in-the-russia-ukraine-war.

[189] Sophia Ankel, "Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up", *Business Insider*, 5 September 2022, https://www.businessinsider.com/ukraine-hackers-create-fake-profiles-russia-troops-share-location-ft-2022-9.

[190] Mehul Srivastava, "Ukraine's hackers: an ex-spook, a Starlink and 'owning' Russia", *Financial Times*, 4 September 2022, https://www.ft.com/content/f4d25ba0-545f-4fad-9d91-5564b4a31d77.

[191] Nataliya Vasilyeva, "Russia blames 'phone scammers' for fire-bombing of enlistment offices", *The Telegraph*, 3 August 2023, https://www.telegraph.co.uk/world-news/2023/08/03/russia-phone-scammers-attack-enlistment-offices-ukraine-war/.

[192] David Kirichenko, "The Growing Importance of Cyberpsychology in Security", *The Close Protection & Security Journal*, December 2023, https://ips-board.org/wp-content/uploads/2023/12/CPSJ-Vol-1-Iss-1-D4-003.pdf.

[193] Daryna Antoniuk, "Ukraine says Russia hacked web cameras to spy on targets in Kyiv", *The Record*, 2 January 2024, https://therecord.media/ukraine-says-russia-hacked-web-cameras-to-spy-on-kyiv-targets.

This footage may have aided Russia in directing drones and missiles during a large-scale strike on Ukraine, including one where nearly 100 drones and missiles targeted Kyiv and Kharkiv.

Since the Russian invasion, the Security Service of Ukraine has blocked around 10,000 cameras potentially used by Moscow for missile strike preparations. Furthermore, an investigation by Radio Free Europe-Radio Liberty (RFE-RL) suggests that Russian intelligence services might have accessed video from thousands of Ukrainian cameras using Trassir, a Russian software capable of tracking movements and recognising faces and license plates. [194]

Impacts on the daily lives of civilians will continue to grow into the future. Just as Russia's cyberattacks on Georgia's banking system in 2008 disrupted daily life, ongoing assaults on Ukrainian critical infrastructure are causing continual disturbances for civilians. Notably, one of the most impactful incidents was the recent attack on Kyivstar. As the world grows increasingly digitised, vulnerabilities multiply, leading to greater opportunities for such disruptions.

Lesson 7: Russia Will Ignore Basic Rules of Cyber War

Prepare for Russia to continue ignoring basic rules of cyber war. Russia violates not only the customary laws of war and international law in its military operations in Ukraine, but it also violates developing cyber norms and international law. Throughout the years, Russia has repeatedly focused its cyber efforts on targeting Ukraine’s critical infrastructure to try and cause chaos without ever seeking to avoid collateral damage to civilian populations. The UK (and the West) must be prepared to handle a revisionist power willing to violate the basic rules of cyber war.

[194] Кирило Овсяний, “Під Наглядом Кремля: Спецслужби РФ Роками Отримували Відео з Тисяч Камер Спостереження По Всій Україні?” *Радіо Свобода*, 7 August 2023, https://www.radiosvoboda.org/a/skhemy-kamery-sposterezhennya-trassir-kreml/32718775.html.

VI. Policy Recommendations

The UK and other Western powers need to be better prepared for this new era in which warfare takes place on digital as well as physical battlefields. These recommendations are designed to support greater resilience, and also to encourage sustained Western support for Ukraine in its cyber defence, an aspect of Kyiv's war against Russian aggression which has received less attention but remains critical, all the more so now the war has become a prolonged, attritional conflict.

Improve coordination between the private and public sectors for shoring up cyber defences. Ukraine was bolstered by the coordination it had established with Western companies and governments that helped keep the country up and running during the initial days of Russia's full-scale invasion. Governments should work hand in hand with private companies to ensure a strong coordination system is in place between the private and public sectors in the event of a major cyberattack or if there is a full-blown cyber war. The private sector plays a crucial role alongside governments, especially in understanding cyber threats, due to its vast data resources. Companies specialising in cyberattack defence hold valuable intelligence that can aid in a threat response.[195] In July 2023, Russian hackers conducted attacks against UK airports; if Russia did manage to bring certain airline operations down, it could cause widespread panic in the country, especially if it takes a long time to remediate any attack.[196] Therefore, Western governments should work on creating a transparent data pool of cyber threats between the private and public sectors. The reality is that a handful of private companies play a critical role in driving large-scale cyber defence.[197] Improving mechanisms of collaboration will be vital for the future.

Invest in creating stronger security mechanisms to protect critical infrastructure. Conduct thorough risk assessments of existing infrastructure systems like bank mainframes and power grids. Many of these systems still rely on outdated technology and legacy systems that may not be equipped to handle modern cyber threats, especially within healthcare and local government.[198] Work with industry experts, government agencies and international bodies to develop and implement new security standards and guidelines. These standards should be adaptable, scalable and able to meet the demands of evolving cyber threats. Ensure that they are applicable not only to new systems but also to existing infrastructure with legacy technology. The UK needs to ensure that security systems are not static. Regular updates, maintenance and audits should be a mandatory part of the cybersecurity protocol for critical infrastructure. The UK Government should also make stronger recommendations to the private sector on focusing their efforts around the 18 CIS Critical Security Controls.[199] However, the recommendations must consider that these infrastructure companies often face challenges due to being understaffed and underfunded. Additionally, there should be investments in prevention mechanisms, such as threat modeling and penetration testing. Organisations should use known attack patterns that Russia has used on Ukraine to define common attack techniques and then use these to harden banking, hospitals, and other critical institutions.

[195] Anushka Kaushik, "Ukraine's cyber defence: Insights on private sector contributions since the Russian invasion", GLOBSEC, 12 June 2023, https://www.globsec.org/what-we-do/publications/ukraines-cyber-defence-insights-private-sector-contributions-russian.

[196] Ryan Daws, "Russian hackers attack UK airports' websites", *Telecoms Tech News*, 20 July 2023, https://www.telecomstechnews.com/news/2023/jul/20/russian-hackers-attack-uk-airports/.

[197] Beecroft, "Evaluating the International Support".

[198] Alex Scroxton, "Critical UK infrastructure a 'hostage of fortune' to ransomware", *Computer Weekly*, 13 December 2023, https://www.computerweekly.com/news/366563154/Critical-UK-infrastructure-a-hostage-of-fortune-to-ransomware.

[199] "The 18 CIS Critical Security Controls", Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-list.

Continue to provide support for Ukraine's cyber defence. Baroness Neville-Rolfe, the UK's lead minister for its conflict stability and security fund, stated that: "The UK and Ukraine are fighting side by side in the cyber war against Russia whose appalling attacks know no bounds. Russia is attacking Ukraine's cyber infrastructure in order to harm innocent people, choke the economy and sow confusion." [200] It cannot be overstated how important Western cyber support has been for Ukraine. As NotPetya showed in 2017, cyberattacks against Ukraine will spill over into the West. Protecting Ukraine's digital infrastructure protects the West.

In October 2023, with support from Estonia, Ukraine built a new cyber classroom that will train cyber military specialists to defend against sophisticated cyberattacks. [201] This is in addition to the military cyber facility Estonia established in 2022 to improve the cybersecurity skills of the Ukrainian military. [202] The cyber lab provides a "training environment to test and strengthen the hands-on skills of military cyber defence professionals with realistic virtual scenarios and real-time simulations that help to identify, monitor and protect from future cyberattacks faster and more effectively." [203] The US and UK should build on these examples from Estonia and invest in training more of Ukraine's military personnel for both cyber defence and offensive capabilities.

Provide Ukraine with more intelligence on Russian vulnerabilities to enable Ukraine to conduct cyber offensives to support its ground campaign. The withdrawal of Western technology from Russia accelerates the pressure on Russian state actors, who may soon face technological debt due to a shortage of essential hardware and software updates, or turn to less-reliable Chinese alternatives. This situation could gradually undermine the security and efficiency of their domestic telecommunications, surveillance infrastructure and advanced cyber research organisations. [204] If Russia keeps using Western tech, it is harder to use zero-day attacks because Western countries don't have a good way to handle them. However, if Western tech is removed from Russia, and it has to use its own or Chinese alternatives, attacking with zero-days becomes easier because there's less worry about accidentally damaging Western systems. We should expect the amount of vulnerabilities, including zero-days, to rise domestically in Russian infrastructure. Ukraine should be given the right tooling and access to vulnerabilities to strike across Russia.

In addition to assisting Ukraine to conduct wider cyberattacks against Russia, such transfer of cyberweapons to Ukraine could also lead to greater Russian pressure to attack Ukraine. If Ukraine (and the West) were willing to take this risk, it could allow Western countries to study how zero-day vulnerabilities will be exploited in future wars, helping them to adapt defensive strategies accordingly. Much as Ukraine was a testing ground for Russian cyberattacks in 2014–2022, Russia could become a testing ground for Western cyberweapons fired by Ukraine.

A few months after the full-scale invasion of Ukraine, Russia threatened that Western cyberattacks on Russia risked a direct military clash and that any attempts to challenge Russia in the cyber sphere would lead to targeted countermeasures from Moscow. [205] Russia said that

[200] Alexander Martin, "Ukraine's partners launch Tallinn Mechanism to amplify cyber support", *The Record*, 20 December 2023, https://therecord.media/tallinn-mechanism-ukraine-partners-cybersecurity.

[201] Joe Saballa, "Ukraine Military Opens New Cyber Defense Training Facility", *The Defense Post*, 10 October 2023, https://www.thedefensepost.com/2023/10/10/ukraine-military-cyber-facility/.

[202] Joe Saballa, "Estonia Builds Ukraine Military Cyber Facility to Fend off Russian Hackers", *The Defense Post*, 12 December 2022, https://www.thedefensepost.com/2022/12/12/estonia-ukraine-cyber-russia/.

[203] "Ukraine: EU sets up a cyber lab for the Ukrainian armed forces", European Union External Action, 12 February 2022, https://www.eeas.europa.eu/eeas/ukraine-eu-sets-cyber-lab-ukrainian-armed-forces_en.

[204] Bateman, Beecroft and Wilde, "What the Russian Invasion Reveals about the Future of Cyber Warfare".

[205] "Russia says West risks 'direct military clash' over cyber attacks", *Reuters*, 9 June 2022, https://www.reuters.com/world/europe/russia-says-west-risks-direct-military-clash-over-cyber-attacks-2022-06-09/.

its critical infrastructure was being targeted by cyberattacks coming from the United States and Ukraine. Despite Russia's vocal threats against the advanced weaponry supplied by the West to Ukraine, such as ATACMS or Storm Shadow missiles, Moscow has similarly refrained from following through on its cyber threats. No one knows where the red lines stand. The fact that increasing the supply of weapons like ATACMS or Ukrainian strikes on occupied-Crimea hasn't caused a strong reaction, even with Putin's strong warnings, suggests the West has been too careful. The same lesson ought to be applied to the cyber domain.

Former General Paul Nakasone, who served as the commander of the United States Cyber Command, underscored the synergy between defensive and offensive cyber operations, stating: "Through persistent presence, persistent innovation, and persistent engagement, we can impose costs, neutralize adversary efforts, and change their decision calculus."[206] Building Ukraine's defences is a win-win for Western governments as they get to use this as a proxy war to validate their own prowess while also understanding the vulnerabilities that they should be testing against in their own systems.

Begin expanding "Hunt Forward" operations with allied nations that are under potential threat. Given the success of the US mission in Ukraine in 2021 prior to Russia's full-scale invasion, Western states should consider a similar approach to countries like Taiwan to protect their critical infrastructure ahead of an invasion.[207] A potential team from the US and UK could help identify vulnerabilities and malicious cyber activity on networks and thwart bad actors before they have the opportunity to execute an attack.[208]

[206] Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine", U.S. Naval Institute, June 2023, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine.

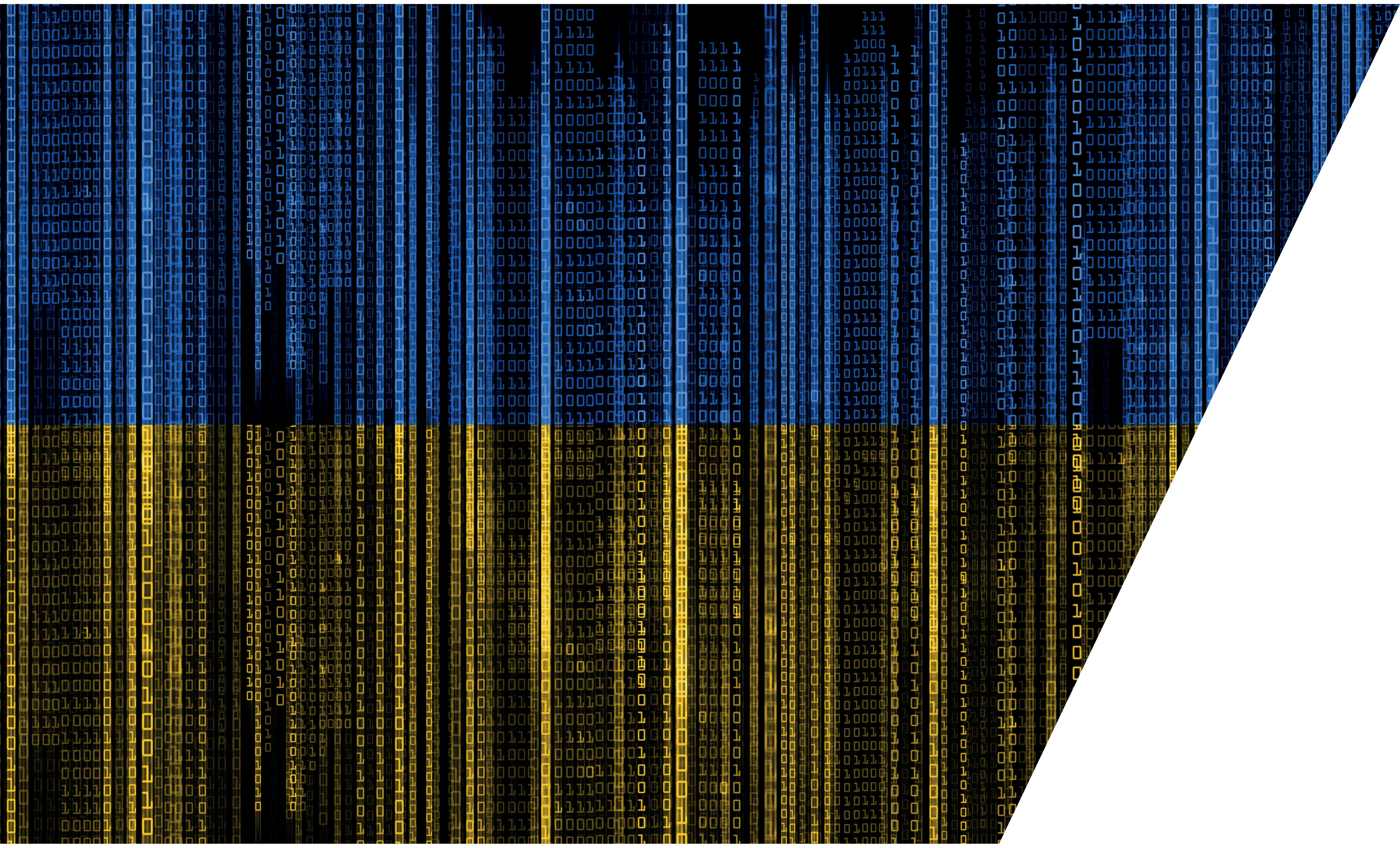
[207] David Vergun, "Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say", U.S. Department of Defense, 3 December 2022, https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/.

[208] Niharika Mandhana, "Ukraine War Shows Difficulty of Large-Scale Cyberattacks, NSA Director Says", *The Wall Street Journal*, 24 March 2023, https://www.wsj.com/articles/ukraine-war-shows-difficulty-of-large-scale-cyberattacks-nsa-director-says-b6bee3b3/.

Title: “LESSONS FROM THE FIRST CYBER WAR: HOW SUPPORTING UKRAINE ON THE DIGITAL BATTLEFIELD CAN HELP IMPROVE THE UK’S ONLINE RESILIENCE”
By David Kirichenko

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org



DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RUSSIA AND EURASIA STUDIES

February 2024