CHAPTER 12

Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War

Kraesten Arnold, Peter Pijpers, Paul Ducheine, & Peter Schrijver

Abstract

The attention to the Russia-Ukraine armed conflict is dominated by the physical devastation it causes. While this seems obvious, the armed conflict is not just a war between two states, but rather a wider conflict where (non-)state actors use numerous instruments of power in various dimensions and domains – including cyberspace – to pursue their interests. Apart from initial success, Russian cyber operations are generally viewed as unsuccessful nuisances, not least due to Ukrainian defences and resilience. Based on an analysis of the current state of cyberwarfare, the authors argue that cyber operations are not just tedious hindrances but also create operational or even strategic impact, hence comply with their purpose.

Keywords: Cyberspace, Russia-Ukraine war, Cyber operations, Digital influence operations, Strategic effects

War is about killing people
and destroying things.[1]

1. (Cyber)war in Europe: An introduction

War is back Europe. However, the Russia-Ukraine armed conflict is not just a war between two states; it is a wider conflict where (non-)state actors use numerous instruments of power in various domains and dimensions to pursue their interests. Although the physical devastation clearly overshadows all other activities, cyberwarfare is definitely taking place.

Multiple destructive cyberattacks supported Russia's military advance before and at the initial stages of the 24th February 2022 invasion. In over a year, a variety of 2776 cyber activities took place.[2] However, due to – *inter alia* – Ukrainian

[1] Freedman, *REAIM Conference Key-Note Speech, the Hague, 15 February 2023.*

[2] Cyber Peace Institute #Ukraine.

resilience and faltering Russian physical operations, cyber operations are generally viewed as unsuccessful. Although the dogs of cyberwar were unleashed, it appears they refrained to bark, let alone bite.[3] That is, at least at first sight.

The war-related cyber operations appear less successful at face value. However, when looking at the objective of such activities, it can be argued that cyber operations did serve their purpose. On 23rd February 2022, Russia attacked the 'Viasat' satellite internet connection, creating a digital vacuum hampering Ukrainian forces and services in their defence.[4] Moreover, the value of 'soft-cyber' or digital influence operations on both sides of the war and of the wider conflict, cannot be overestimated. These activities go well beyond the Ukrainian battlefield.[5] Whereas Russia has to hush domestic audiences and prevent its population from turning against the war or the regime, Ukraine needs to engage its allies in the free world. For Ukraine, international support is its lifeline and thus the centre of gravity, but consequently also its Achilles' heel.

This chapter addresses what kind of (cyber)war was envisaged and what sort of cyber activities and effects were actually observed on both sides.[6] This analysis will be preceded by a brief perspective on the utility of cyberspace for military operations in general and an overview of the different types of military operations in the information environment. The penultimate section will attempt to determine whether Russia's cyber-offensive failed or Ukraine's defences prevailed, and to assess the strategic value of the various types of operations. This chapter concludes with a view to future conflicts.

2. The utility of cyberspace for military operations

With the dawn of cyberspace, including the Internet and its social media platforms, our societies have become ever more digitalised. Digital processes in all its forms have become the nervous system facilitating everyone's daily life. Individual citizens, companies or governments utilise this digital interconnectedness

[3] Kostyuk and Gartzke, "Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine." The phrase related to the dogs of war stems from Shakespeare's Julius Caesar.

[4] Kaspersky Lab, "Evaluation of cyber activities and the threat landscape in Ukraine takeaways from Kaspersky for international discussions on stability in cyberspace."

[5] Bateman, "Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications," 43-44; Helmus, "The Ukrainian army is leveraging online influences. Can the U.S. military?"

[6] Based on the sources available. Not all variances in CEMA-operations were observed or reported on during the war, e.g. EW operation or hard-cyber operation from the Ukrainian side.

incorporating a growing range of objects and services for numerous facets of life and society.[7]

While there are many communicative and commercial benefits, our digitised society is both a blessing and a curse.[8] All of these facets and objects have become susceptible and vulnerable to exploitation. Digital data and interconnectivity facilitate intelligence-gathering in enormous amounts over long distances. Furthermore, malign actors may abuse the attributes of social media and penetrate the very capillaries of our society to target specific audiences and spread toxic disinformation, or merely withhold information and give alternative views. Not only transboundary, but also within national boundaries to control one's citizens.[9]

Thus, both benevolent and malicious social interaction entails an ever-larger digital composite, to the extent that some social interaction is 100% digitalised. Unavoidably, warfare, being a rare niche exponent of social interaction, will become digitalised as well. The fact that by now some thirty odd states have established cyber commands within their armed forces, supports this expectation.[10]

Of old, military operations were conducted in the physical dimension (such as the Battle of Waterloo) as well as in the cognitive dimension. The latter often combining physical and cognitive elements into classic deception operations such as the Trojan Horse and WWII's Operation Mincemeat, and the modern 2014 Green Men in Crimea.

With the inception of modern technology new proponents of physical operations – such as electronic warfare (EW) using a facet of the physical dimension, i.e., the electromagnetic spectrum – supplemented the classic or well-known repertoire. With the inception of digital technology, a virtual dimension came to avail, leading to the development of cyber operations alongside EW. Nowadays, cyber and electromagnetic activities (CEMA) are often named together as complementary action (see Figure 12.1).

Ultimately, activities in a conflict or competition are meant to impose one's will on opponents or audiences by leveraging or supporting a cognitive, virtual or physical effect – directly or indirectly. This is achieved through actions or operations in the cognitive, virtual and/or physical dimension: i.e. by manoeuvring,[11] and the

[7] Haaster, "On cyber: The utility of military cyber operations during armed conflict"; Keulen, "Digital force : Disrupting life, liberty and livelihood in the information."

[8] Smeets, "The Strategic Promise of Offensive Cyber Operations," 105.

[9] Lam, "The People's Algorithms: Social Credits and the Rise of China's Big (Br)Other," 81-84; Shires, The Politics of Cybersecurity in the Middle East.

[10] Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.*

[11] Pijpers and Ducheine, "'If you have a hammer': Shaping the armed forces' discourse on information maneuver," 1165-1167.

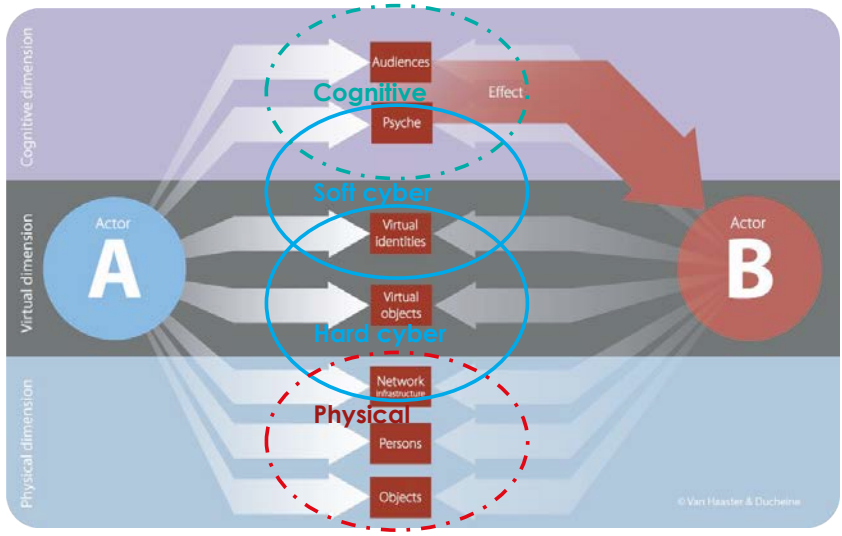

Figure 12.1: Operations in the information environment

result of a longer process; whether undertaken by a joint force, land, sea, or air, or by another agency (such as an intelligence & security service).

The prerequisites for these operations or activities are intelligence and understanding. By observing the cognitive, virtual and/or physical dimension, situational awareness and understanding is gained.[12] This understanding is fed into the (rest of the) planning and the decision-making process (Figure 12.2).[13] Once a decision is made, coordination and orchestration are required to task troops. This is part of the command and control process. Thereafter, action is taken, and results are observed and evaluated. This generic process (observe, understand, decide, orchestrate, act) resembles the OODA-loop[14] and is described in modern publications on i.a. Multi-Domain Operations.[15]

Thus, cyberspace facilitates digital intelligence gathering into virtual capabilities, among others through scanning or copying data confined in virtual repositories. In addition, it offers insight into motives and sentiments through analysis and roaming virtual expressions. Moreover, in a digitised society, many

[12] DCDC, "JDP 04 2nd Edition – Understanding and decision-making."

[13] Pijpers and Ducheine, "'If you have a hammer': Shaping the armed forces' discourse on information maneuver," 1169-1170.

[14] Osinga, "Science, strategy and war: The strategic theory of John Boyd."

[15] United Kingdom Ministry of Defence, "Multi-domain integration (Joint Concept Note 1/20)."

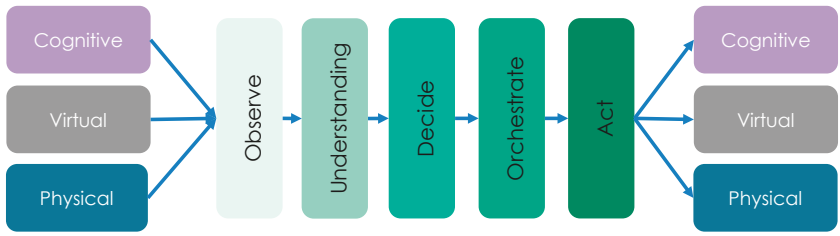

Figure 12.2: Manoeuvring in the Information Environment

physical objects can be tracked or accessed via cyberspace offering insight into the location and/or status of equipment or services.

For the purpose of this chapter, and as they are described elsewhere in this volume, intelligence activities will not be included.[16] Given the cyber-related scope of this chapter, physical activities (e.g. airstrike or ground forces assault) will not be covered here either.

To assess the potential effect of CEMA in the Russia-Ukraine war, a conceptual frame is provided on activities and effects. Ducheine et al.[17] argue that the dawn of cyberspace has invigorated existing activities, but also enabled a new one. Apart from digital intelligence gathering, activities involving the use of cyberspace can entail (i) cognitive or influence operations using cyberspace as a vector,[18] and target the cognitive dimension, entailing content, words, memes and footage as a 'weapon.'[19] New are the (ii) virtual operations that undermine or subvert cyberspace itself ('hard cyber operations') with binary code, in order to modify or manipulate data, and to degrade or destroy the ICT infrastructure, resulting in (virtual and/or physical) effects *in* cyberspace. As communication via cyberspace (both cabled and wireless) is highly dependent on the electromagnetic spectrum, (iii) physical Electronic Warfare (EW) can be used to undermine the use of drones, artillery and command and control systems.[20]

[16] For the intelligence dimension of the Russia-Ukraine war, see Chapters 3, 4 and 5.

[17] Ducheine, Haaster, and Harskamp, "Manoeuvring and generating effects in the information environment"; Pijpers and Arnold, "Conquering the invisible battleground"; Ducheine, Arnold, and Pijpers, "Decision-making and parliamentary control for international military cyber operations by The Netherlands Armed Forces."

[18] Whyte and Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, 100-101.

[19] Lupion, "The gray war of our time: Information warfare and the Kremlin's weaponization of Russian-language digital news," 329-330; Walton, "What's old is new again: Cold War lessons for countering disinformation"

[20] Theohary and Hoehn, "Convergence of cyberspace operations and electronic warfare effects."

The potential and actual impact of cyber activities is widely debated; some scholars argue that cyberwarfare will equal regular warfare,[21] while others argue that cyber means will never reach the threshold of war.[22] Since most cyber operations, whether during an armed conflict or beyond, will not reach the threshold of force, labelling these cyber operations based on their effects might be more appropriate.[23] Gartzke & Lindsay state that cyber activities, such as digital influence or hard cyber operations, have the effect of mere hindrances or nuisances. They may support campaigns in other (i.e. land, sea, air, space) domains, or could have a strategic impact.[24] While a strategic effect is possible in theory, they shelve it as a myth.[25]

Another take on the impact of cyber operations is articulated by Smeets (& Harknett) stating that cyber activities can be enablers or force-multipliers for conventional capabilities or a strategic alternative to war, hence an independent asset achieving strategic outcomes without the need of armed attack. Strategic in this sense means that the intent of the operation is 'to shift the relative balance of national power among states.'[26] Smeets makes a distinction between cyber capabilities countering values and countering force.[27] The former includes targeting national assets which can include vital infrastructure such as the 'Stuxnet' attack,[28] while the latter involves targeting operationally relevant assets including the attack on Syria's Air Defense System with the 'Suter program'[29] or a distributed denial-of-service (DDOS) attack.

Based on the academic discourse above, three main effects of cyber operations can be distinguished (Figure 12.3). Firstly, the cyberattack with a severe strategic impact changing the balance of power between states. Examples would be the manipulation of nuclear command and control systems or 'disconnection from the Internet.' Strategic cyber operations with such far-reaching consequences have not

[21] Stone, "Cyber war will take place!"

[22] Rid, "Cyber war will not take place"; Valeriano, "War is still war: Don't listen to the cult of cyber."

[23] Smeets, "The strategic promise of offensive cyber operations," 90; Harknett and Smeets, "Cyber campaigns and strategic outcomes," 558.

[24] Lindsay and Gartzke, "Coercion through cyberspace: The stability-instability paradox revisited," 179-203.

[25] Gartzke, "The myth of cyberwar: Bringing war in cyberspace back down to earth."

[26] Harknett and Smeets, "Cyber campaigns and strategic outcomes," 535.

[27] Smeets, "The strategic promise of offensive cyber operations," 93-96.

[28] Referring to Operation Olympic Games ascribed to the US' and Israel's effort to sabotage Iran's nuclear program (2007-2010). Sources: Robert Langer 'To kill a centrifuge' and David Sanger *Confront and Conceal*.

[29] Referring to the Israeli 2017 Operation Orchard, see for example Soesanto, "A digital army: Synergies on the battlefield and the development of Cyber- Electromagnetic Activities (CEMA)," 29-30.

yet been witnessed, although the 2010 Operation 'Olympic Games' (a.k.a. Stuxnet) that targeted an Iranian uranium-enrichment facility, or the cyber operations that affected the 2016 US presidential elections may come close. Secondly, cyberattacks that support operational level military or even diplomatic campaigns. Intelligence and reconnaissance operations (or 'cyber espionage') to support military operations are obvious examples.[30] Other supportive operational level cyber activities could involve 'ransomware' and 'wiperware'; malicious software aimed at data encryption and/or data destruction respectively. Supportive cyberattacks also include manipulation of parts of the Internet. Thirdly, cyberattacks depicted as nuisances, neither causing 'death and destruction' nor directly supporting a military campaign, and without strategic impact. Prominent examples thereof are DDoS-attacks, defacements, phishing and hack-and-leak operations. Furthermore, these cyber-hindrances may also encompass mobilising support (via social media), calling for resistance, libeling and defaming.

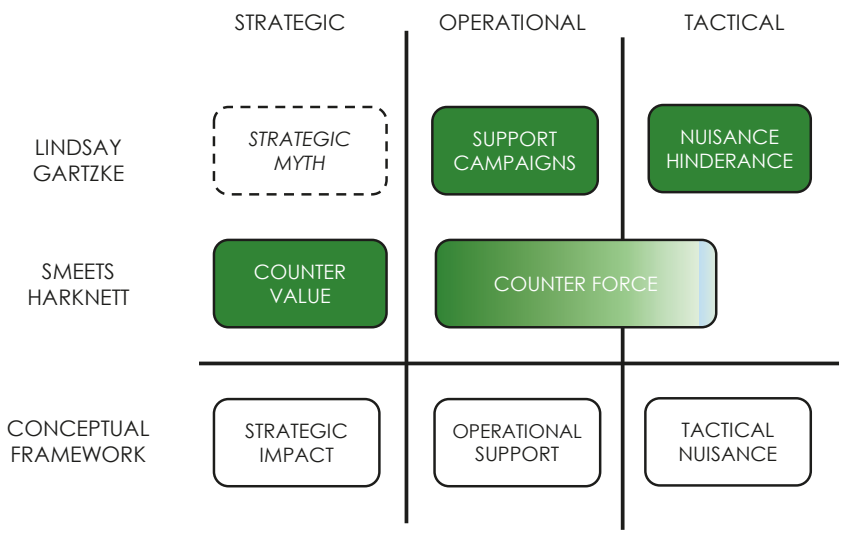

Figure 12.3: Effects of cyber operations

[30] Bowen, "Russian cyber units."

3. The expected cyberwar

For many (outside of Ukraine), the Russian 2022 invasion in Ukraine came as a surprise. Maybe not that it happened at all – the conflict had been boiling for a decade – but rather the manner in which it escalated.

The envisioned war was thought to resemble a cyber equivalent of the Russian annexation of Ukraine's Crimea in 2014.[31] Instead, Russia used brute physical force violating the sovereignty of Ukraine and breaching the peremptory rule of the prohibition of the use of force. Quite different from previously more sophisticated and subtle Russian operations to curb the will of its opponents, such as during the 2015 and 2016 cyber operations crippling Ukraine's power system, or the 2017 'NotPetya' cyberattack on the Ukrainian fiscal system.[32]

The question is, whether this expectation of a cyberwar was a valid one, or not.[33] For academics, a crucial moment of self-reflection. After introspection and validation, based on the digitised state of modern society, Russia's intentions and cyber track record, as well as the trend to establish cyber commands within armed forces worldwide, the expectation seemed fair and valid.

3.1 Russian intentions

With the inception of cyberspace, a new arena of engagement was added. According to Rid,[34] Russia has embraced the digitalisation of the information environment to refine its 'Active Measure'-doctrine. Russian Active Measures rely on manipulative influencing techniques referred to as reflexive control[35] i.e., 'conveying to a partner or an opponent specially-prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.'[36]

Since the presidency of Vladimir Putin, Russia's intent has been to challenge the Western dominance and offer an alternative view on international relations and law.[37] Moreover, Putin argues that Russia is a global power that needs to be reck-

[31] Polyakova and Boyer, "The future of political warfare: Russia, the west, and the coming age of global digital competition the new geopolitics," 1.

[32] Soldatov and Borogan, "Russian cyberwarfare : Unpacking the Kremlin's capabilities," 22-29; Baezner and Robin, "Cyber and information warfare in elections in Europe," 6-7.

[33] Pijpers, Ducheine, Arnold, "The next war would be a cyberwar, right?"

[34] Rid, "Disinformation: A primer in Russian active measures and influence campaigns."

[35] Thomas, "Russia's reflexive control theory and the military," 238-243.

[36] Ajir and Vailliant, "Russian information warfare : Implications for deterrence theory," 72-73; Giles, "Handbook of Russian information warfare," 19.

[37] Zaporozhchenko, "The end of 'Putin's Empire?' Ontological problems of Russian imperialism in the context of the war against Ukraine, 2022."

oned with, seeking Western confirmation thereof. Finally, Russia as a global power wants to have a buffer zone with nemesis NATO. This zone – or sphere of influence – includes Belarus, Ukraine and Georgia.[38] Russia challenges Western states not by advocating authoritarian regimes but by undermining the, in their view, Western feeble, hypocritical liberal democracies they despise.[39] Disseminated alternative truths generate strategic confrontation and confusion.[40] The intent of digitalised Active Measures is that Western audiences start to doubt Western truisms.

3.2 The prelude to the Russia-Ukraine war

After the Cold War and the demise of the Soviet Union, Russia slowly increased its influence in its Eastern and Southern buffer zones, initially via military means. However, after the mishap in the 1st Chechen war and Putin's rise, the policy was expanded to include diplomatic (involving like-minded local leaders),[41] informational and cyber-means.

To keep Ukraine within its sphere of influence, instead of leaning towards the EU, Russia attempted to interfere in Ukraine's 2014 presidential elections. Using state and proxy agents, it subsequently annexed Crimea, occupied parts of the Donbas area, and conducted destructive cyberattacks resulting in energy outages in 2015 and 2016 and worldwide devastating financial losses and logistical stagnation resulting from the use of NotPetya against one of Ukraine's fiscal IT services in 2017.[42]

Given the Russian exploration and experiences of 'warfare' in the information environment and cyberspace, it was expected that future conflicts or wars would have a substantial cyber component;[43] if not an all-out cyberwar. *Prima facie* however, the Russia-Ukraine war did not meet that expectation. Was the impact of cyberwarfare misjudged or did it not yet come to fruition?

[38] Flockhart and Korosteleva, "War in Ukraine: Putin and the multi-order world," 472-475.

[39] Hansel, "Great Power narratives on the challenges of cyber norm building," 190.

[40] Black, "Russia's war in Ukraine : Examining the success of Ukrainian cyber defences," 10; Pijpers, "Influence operations in cyberspace: On the applicability of public international law during influence operations in a situation below the threshold of the use of force," 49.

[41] Galeotti, *Putin's Wars: From Chechnya to Ukraine*.

[42] Polyakova and Boyer, "The future of political warfare: Russia, the West, and the coming age of global digital competition the new geopolitics," 14.

[43] Schulze and Kerttunen, "Cyber operations in Russia's war against Ukraine," 3-4.

4. How Russia-Ukraine cyberwarfare evolved

Often only the most severe cyberattacks are registered and analysed.[44] In the Russia-Ukraine war few cyberattacks hit the headlines. It appears that aside from the eye-catching Viasat-attack very little happens in cyberspace.[45] The reality is to the contrary.

Operations in and through cyberspace entail a variety of 'cyberattacks' including hard cyber operations and digital influencing operations or soft-cyber operations. Complemented by EW, these cyber operations aim to have a strategic effect, to support operational (military) campaigns or to cause mere hindrance of tactical/local effects. Based upon this conceptual frame, we assess the observed cyber activities in the Russia-Ukraine war, considering the numbers and impact of the cyber operations and their evolution over time from February 2022 to June 2023.

4.1 Ukraine's preparations and defences

In anticipation of predictable Russian cyberattacks,[46] prior to the actual invasion, Ukraine increased its resilience in cooperation with the US and the UK (initially on-site and later remotely)[47] and a variety of commercial high-tech companies (e.g. Microsoft, Mandiant, ESET, Amazon Cloud Services).[48] Thus, active incident response and information sharing between Ukraine, IT-security firms, and the allied network defenders severely disrupted Russia's destructive cyberattacks.[49]

4.2 Russian hard cyber operations

In the immediate run-up to the February 2022 invasion, pro-Russian hackers executed rather straightforward denial-of-service attacks to impede the access of the Ukrainian Ministry of Defense, the armed forces, internet service providers and two national banks.[50] In that period, hackers also defaced the websites of dozens of

[44] Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*.

[45] Mironova, "Russia's invasion of Ukraine is also being fought in cyberspace."

[46] Weymouth, "Volodymyr Zelensky: 'Everyone will lose' if Russia invades Ukraine"; Sonne, Ryan, and Hudson, "Russia planning potential sabotage operations in Ukraine, U. S. Says."

[47] Martin, "US military hackers conducting offensive operations in support of Ukraine, says Head of Cyber Command."

[48] Bateman, "Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications," 14.

[49] Microsoft Threat Intelligence Centre, "A year of Russian hybrid warfare in Ukraine," March 15, 2023, 5.

[50] Ukrainian Centre for Strategic Communication, 15 February 2022.

Ukrainian government organisations with manipulated political imagery and provocative propaganda messages.[51] Spear-phishing mails targeted Ukrainian entities to divulge sensitive data. Although annoying, these many hundreds of cyberattacks had only modest impact.[52]

Mid-January 2022, Microsoft revealed the existence of a malware operation targeting multiple organisations in Ukraine.[53] This 'wiperware' (dubbed *Whispergate*) masqueraded as 'ransomware' but had no intention of locking data for a ransom. Instead, this malware basically erased (wiped or overwrote) data on the victims' computers and subsequently destroyed the computers' start-up mechanism intending to render these machines useless.

One day prior to the invasion, cybersecurity firms revealed the detection of more 'disk-wiping' malware, targeting hundreds of machines in Ukraine in the financial, defence, aviation, and IT-services sectors.[54] To date, at least nine different destructive wiper-families and two types of ransomware targeted the Ukrainian government, critical infrastructure, media, and the commercial sector.[55] It is striking that these wipers coincided with the immediate lead-up to the invasion and the few months thereafter. It is possible that these cyberattacks were conducted largely in concert with the kinetic military operations.[56] This is fully in line with the importance that Russia attaches to decisive impact during the first weeks of a war.[57]

An event with far-reaching consequences and coinciding with the complementary cyberattacks against Ukrainian internet service providers and telecommunication services, concerned a cyberattack with yet another kind of wiperware (*AcidRain*) on Viasat, a major satellite internet communications provider for, among others, Ukraine and other parts of Europe. On the eve of the invasion, hackers erased the hard drives of Viasat's associated satellite internet homebased modems rendering these unserviceable. This resulted in the loss of battlefield communications particularly in the region close to the then seriously threatened Kyiv, making Ukrainian forces virtually blind to Russian troop positions and movements.[58]

[51] Security Service of Ukraine, "Cyber attacks on government websites."

[52] Kostyuk and Brantly, "War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation," 498.

[53] Microsoft Threat Intelligence Centre (MSTIC), "Destructive malware targeting Ukrainian organizations."

[54] Symantec Threat Hunter Team, "Ukraine: Disk-wiping attacks precede Russian invasion."

[55] MSTIC, "A year of Russian hybrid warfare in Ukraine."

[56] Smith, "Defending Ukraine : Early lessons from the Cyber War," 3.

[57] US Defense Intelligence Agency (DIA), Russian military strategy: Core tenets and operational concepts, 3; See also: Lin, "Russian cyber operations in the invasion of Ukraine."

[58] Blessing, "American Enterprise Institute, revisiting the Russian Viasat hack: Four lessons about cyber on the battlefield."

The cyberattack on Viasat is a good example of how cyberattacks can be targeted and timed in operational support of military operations by disrupting and destroying the technology used by enemy forces.[59] Thanks to the personal relationship between Ukraine's minister for Digital Transformation Mykhailo Fedorov and Elon Musk,[60] the latter's Starlink satellite system quickly filled the incurred gap and restored Ukraine's internet communications.[61]

In spring 2022, Russia withdrew the forces advancing toward Kyiv and redirected these to focus on other regions. Simultaneously, a shift in pro-Russian cyberattacks to the logistics and transportation sector inside Ukraine was observed.[62] At that time, Ukraine's railways and transportation systems transferred weapon systems and military supplies eastward. Refugees used these means to flee in the opposite direction. Russian forces launched both missile-strikes and destructive wiper-attacks on the transportation infrastructure, suggesting a common goal.

In April, hackers targeted the Industrial Control Systems of a critical infrastructure: the Ukrainian power grid. The attacker had modified the previously used (2016) *Industroyer* malware to attack the power grid and cause power outages. Although similar to its predecessor, this version contained more targeted functionality. In addition, it was accompanied by yet other sets of destructive wiper malware.[63] Late 2022, following Ukraine's military successes in regaining control over southern and north-eastern territory, Russia started kinetically attacking civil critical energy infrastructure. Given the diversity of the target infrastructure and the required access positions necessary for cyber activities, it is suggested that the generic capabilities and quick reaction times favoured kinetic action over tailored cyber actions. With the winter in sight, power and heat infrastructure were hit by numerous missile strikes. Concurrently, and possibly in support of these kinetic operations, wiper malware attacks targeted civilian power and water infrastructure.[64]

In contrast to kinetic military operations, cyber operations can be executed covertly and, hence, are more suitable to be conducted in areas outside Ukraine. Pro-Russian actors used (*Prestige*) ransomware to attack the transportation sector in Ukraine and Poland, a NATO-member and a logistical hub for supplies.[65]

[59] O'Neill, "MIT Technology Review, Russia hacked an American satellite company one hour before the Ukraine invasion."

[60] Musk, "Starlink service is now active in Ukraine," *Twitter*, 2022.

[61] Jin, "Musk says Starlink active in Ukraine as Russian invasion disrupts internet."

[62] Microsoft Threat Intelligence, "A year of Russian hybrid warfare in Ukraine, What we have learned about nation state tactics so far and what may be on the horizon."

[63] ESET Research, Industroyer2: Industroyer reloaded, 12 Apr 2022.

[64] Watts, "Preparing for a Russian cyber offensive against Ukraine this winter."

[65] Microsoft Threat Intelligence Centre (MSTIC).

In the course of 2022, the deployment and intermittent introduction of new wiper variants took place in waves. This suggests that the attackers were forced to react (and improvise), rather than draw prepared cyber weapons from a stock. Over time, the technical level of the wipers declined.[66]

4.3 Russian electronic warfare

Prior to the invasion, some Western analysts had expressed admiration for Russia's military EW capabilities. However, certain events cast doubt on their actual strength and readiness.[67] Initially, Russia's EW complex has proved partially successful in suppressing Ukrainian air defence assets, which cleared the way for an air assault operation on Hostomel airfield near Kyiv.[68] However, this success was not sustained in the weeks thereafter.

Ukrainian Unmanned Aerial Systems (UAS), like the Bayraktar TB-2, freely roamed and targeted Russian convoys north and east of Kyiv without significant interference by Russian EW-systems.[69] Arguably, this was attributed to a lack of planning for the invasion that resulted in ineffective deployment of EW systems.[70] Following the failed attempt to capture Kyiv, frontlines stabilised more or less in the south and the east. That paved the way for more effective Russian EW-operations from static positions, specifically in the execution of target acquisition in tandem with UAVs.[71] Likely due to denser Russian electronic defences, Ukraine's initial success with the UAS Bayraktar was not continued. Nonetheless, cheaper commercial and expendable drones continued to provide Ukrainian forces with critical battlefield awareness for targeting purposes.[72]

Russian attempts to block Ukrainian communications, similarly, largely failed. Not least due to the large-scale delivery of the Starlink satellite communications architecture. This allowed Ukraine to maintain dependable connections throughout tactical formations, with limited to no interference from Russian electronic warfare assets.[73]

[66] https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak.

[67] McDermott, "Russia's electronic warfare capabilities to 2025," 2.; Withington, "Russian EW: Underused or a Potemkin capability?"

[68] "The Russian air war and Ukrainian requirements for air defence," 7.

[69] Idem.

[70] Watling and Reynolds, "Ukraine at war: Paving the road from survival to victory," 10.

[71] Idem.

[72] Army, "6. Explosives delivered by drone."

[73] Colom-Piella, "The bear in the labyrinth," 77.

4.4 Russian digital influence (soft-cyber) operations

Next to the aforementioned EW and hard cyberattacks, pro-Russian state and non-state actors conducted cyber-enabled operations – disruptive propaganda, and disinformation campaigns (both mainstream and social media) – to influence target audiences.[74] False narratives were distributed via government-managed and influenced websites (e.g., RT and Sputnik), amplifying aligned framed messages,[75] propaganda and disinformation spreading through exploited social media services.[76]

The main purpose of Russian influence operations is to demoralise the Ukrainian population, and to drive a wedge between Ukraine and its Western allies. The integrity of Western states was undermined by a report on bioweapons made in Ukraine, alluding to the hypocrisy and decadence of the West.[77] Influence operations are also used to target domestic Russian audiences, Russian diaspora. Narratives used are Western Russo-phobia, a sensitive topic to Russian diaspora or ethnic Russians living in Ukraine, the 'denazification and demilitarization' of Ukraine or the endemic corruption within the Ukrainian government.[78]

4.5 Ukrainian digital influence (soft-cyber) operations

Ukraine too exploits the social media. From the invasion on, President Zelensky addresses his population online and keeps up the morale of his troops,[79] affecting the cognitive dimension of both friend and foe. The story of a Ukrainian fighter pilot, 'the Ghost of Kyiv,' went viral online. The pilot allegedly shot down six Russian aircrafts on the first day of the invasion. While the Ukrainian Air Force Command admitted that the Ghost of Kyiv did not exist, the virtual myth lives on. Another occurrence concerned the bold response of Ukrainian troops defending Snake Island after Russia's Black Sea Fleet flagship 'The Moskva' demanded their surrender. The explicit refusal 'Russian warship, go home'[80] became a popular

[74] Kleisner and Garmey, "Tactical TikTok for Great Power competition – Applying the lessons of Ukraine's IO campaign to future large-scale conventional operations," 12-14.

[75] See inter alia: the website donbasstragedy.info (created 26 Nov 2021) and pushing posts containing "Kyiv has begun to create a "human shield" of the civilians of Donbass" on 24 Feb 2022.

[76] Microsoft, "Defending Ukraine: Early lessons from the Cyber War," June 22, 2022, 4.

[77] Ling, "How U.S. bioweapons in Ukraine became Russia's new big lie"; EU vs Disinformation, "Weapons of mass delusion."

[78] Lichtenstein et al., "Framing the Ukraine crisis: A comparison between talk show debates in Russian and German television," 66–88.

[79] "We are here to defend our independence" Zelensky, 25 February 2022, https://m.youtube.com/watch?v=WkNiYYzHeDs

[80] The actual phrase was (translated into English) "go f**k yourself," see The Guardian.

phrase online and was frequently used in internet memes. A stamp was subsequently introduced to honour the heroes. The Moskva's sinking created the theme for another postage stamp and new online memes, as did the attack on the Kerch Bridge (Ill. 12.1).

Illustration 12.1: Meme stamp of the Kerch Bridge

Of strategic importance is the fervent on-line strategic communication by Zelensky to foreign parliaments that result(ed) in diplomatic support and, moreover, in the supply of funds, military systems and ammunition.

Further, the online presence of Ukrainian state institutions, units of the armed forces, and volunteer organisations is ubiquitous. It is noteworthy that social media publication policies are part of a strategic communication engagement, guided from Kyiv, ensuring that messaging revolving around bravery, resilience, and defiance is consistent and aligned with overarching goals.[81] Within these guidelines, content creators hardly face restrictions.[82]

Humorous content and interaction with animals, particularly cats and dogs, are recurring themes in videos of Ukrainian units on social media.[83] Additionally, blatant failures and alleged crimes of Russian armed forces are frequently emphasised.[84] Other topics, such as the heroism of military personnel, martyrs (although

[81] Interview with Ukrainian Lt. Col. The transcript is accessible via the authors.

[82] BBC news, "How Ukraine is winning the social media war."

[83] News Week, "Ukrainian soldier's "cat checkpoint" delights internet."

[84] Hogue, "Civilian surveillance in the war in Ukraine: Mobilizing the agency of the observers of war," 109.

there is no publication of overall casualty numbers), and a promotion of home-grown (drone) technology, are also commonly featured.[85]

In this way, and as of the first day of this war, social media has helped Zelensky to internationalise Ukraine's cause and to persuade (Western) democratic countries to support his country.

5. Assessing cyber activities: Failed offensive or successful defence

The role of cyber operations in the Russia-Ukraine war differs from what was expected. Apart from the invasion related attack on Viasat and the coinciding (wiperware) attacks on ISPs and telecommunication providers (TelCo) providers, hard cyber operations (digitally undermining cyberspace) that effectively supported military campaigns were unexpectedly sparse. The majority of the activities related to hindrance such as DDoS and spear-phishing attacks.

5.1 Strategic value?

Quite interesting are the wipers that have been used. In the first year of the war, nine variants of wiperware have been deployed against mainly civilian objects of the Ukrainian government, critical infrastructure (information technology, communication, energy, transport, healthcare), the commercial businesses and the media. A small percentage was directed against the armed forces.[86]

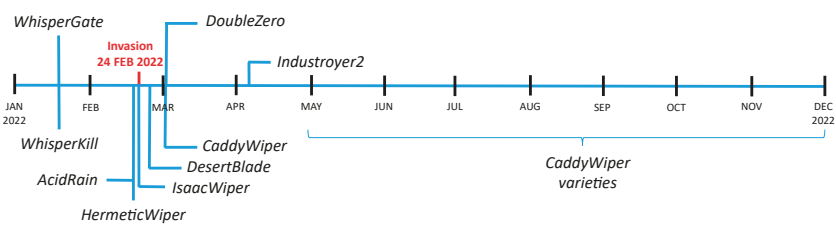

Figure 12.4 (Discovery of) Nine wiperware-families deployed around the Russion invasion

It is striking that these wipers were mainly deployed in the run-up to the invasion and the few weeks thereafter (figure 12.4). It stands to reason that the use of wipers

[85] Alshamy et al., "Polycentric defense, Ukraine style: Explaining Ukrainian resilience against invasion," 18.

[86] Microsoft Threat Intelligence Centre, *A Year of Russian Hybrid Warfare in Ukraine*.

served as operational support to the military campaign in shaping the battlefield – a counter force asset to blind Ukraine's defences. It can even be argued that when targeted at critical infrastructures, wipers strike the vital interests of Ukraine. Following the categorisation by Smeets,[87] during the Russia-Ukraine war, these wipers could have had a potential strategic impact, but based on the data at hand, we cannot convincingly conclude that they actually had.

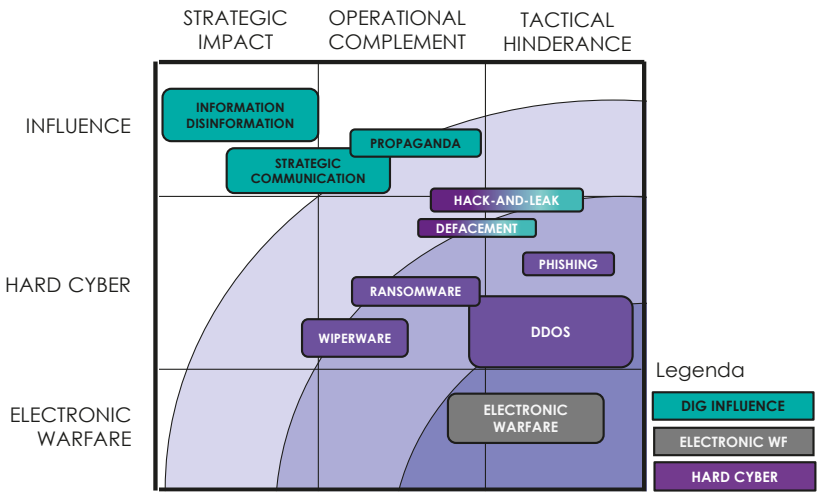

Figure 12.5 Cyber & electomagnetic attacks in the Russia-Ukraine war

Digital influence (soft cyber) operations, especially the mobilisation of support, were initially categorised as a minor hindrance. However, during the current war (manipulative) digital influence operations from both Ukrainian and Russian state entities proved to have generated (and strived for) strategic effects (Figure 12.5) as international support developed into the centre of gravity for both.[88] For Ukraine it resembles the lifeline to stay afoot. All Russia has to do is to weaken this Achilles' heel.

The Russian cyber operations in January and February 2022 should be regarded as a success. Through the hacks against satellite internet communications provider Viasat, telecom and internet service providers, and e-services, Russian operators or their affiliates, were able to create a digital blackout. One symptom of this blackout was Fedorov's tweet to Elon Musk, requesting Starlink to enable communications.

[87] Smeets, "The strategic promise of offensive cyber operations," 95.

[88] See also: Beskow, Hawthorne, and Daniel, "How to win with data: The US SOF-cyber partnership supporting Ukraine."

Nevertheless, although cyber activities had a strategic impact in the first days of the war, and a vast number of cyber activities were recorded,[89] thus far Russia's war-related cyber campaign appears ineffective to most observers. This raises the question: Is Ukraine's defence formidable or is Russia's cyber force failing?

5.2 Ukraine's defence

It is realistic to acknowledge that information on Russia and Ukraine is limited or biased. Ukraine might withhold information about successful Russian attacks for reasons of operational security or to uphold the morale of its population and forces. Apart from that, Ukraine's cyber defence is well organised,[90] and attacks were intercepted.[91] Over the years,[92] Ukrainian cyber infrastructure including the telecommunications sector has been hardened by domestic, international (US, UK)[93] and commercial (such as Microsoft) support cushioning the impact of an attack. Ongoing cyberattacks since the annexation of Crimea have, unintentionally transferring knowledge,[94] given away Russia's *modus operandi* in advance.

Furthermore, preparation for the war by Ukraine's telecommunications sector paid off. Anticipating the invasion, mobile telecom provider Kyivstar disabled incoming roaming devices from Russia and Belarus.[95] This prevented Russia's military leadership using mobile devices as alternates for their flawed command and control setup during the chaotic first weeks of the invasion. Instead, Russian officers had to resort to confiscated Ukrainian phones, exposing themselves to surveillance and subsequent targeting.[96] Ukrainian providers placed priority on repairing damaged telecom infrastructure, which enabled C2 redundancy for the Ukrainian military. This enhanced the population's resilience, still able to contact their relatives in these chaotic times.[97] The vast majority of Ukraine's population owns a mobile phone.[98] Consequently, the state was able to continue communication

[89] Cyber Peace Institute, "Cyber dimensions of the armed conflict in Ukraine."

[90] Cerulus, "Kyiv 's hackers seize their wartime moment"; Black, "Russia's war in Ukraine : Examining the success of Ukrainian cyber defences," 12-15.

[91] Based on threat intelligence advances, supported by artificial intelligence, and internet-connected end-point protection. See: Smith, "Defending Ukraine: Early lessons from the Cyber War," 2.

[92] Beecroft, "Evaluating the international support to Ukrainian cyber defense."

[93] Fleming, "The Head of GCHQ Says Vladimir Putin Is losing the information war in Ukraine."

[94] Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.*

[95] "The mobile network battlefield in Ukraine – Part 1."

[96] Dalsjö, Jonsson, and Norberg, "A brutal examination," 13.

[97] "The mobile network battlefield in Ukraine – Part 1."

[98] "Mobile cellular subscriptions (per 100 People) – Ukraine | Data."

with its citizens through the e-government app '*Diia.*'[99] Furthermore, the state provided an air raid alarm system through mobile phones and an *'eVorog'* (enemy reporting) app, which helped to improve security and facilitated the crowdsourcing of intelligence.[100]

In areas where connectivity was no longer available due to destruction of internet and telecom infrastructure, or Russian denial of the electromagnetic spectrum (EMS), innovative technologies guaranteed continued command and control capabilities of Ukraine's military. Commercial US company Starlink emerged as the backbone of the Ukrainian reconnaissance fire complex (designed for the coordinated employment of fires), comprising UAS and indirect fire assets.[101] Using Starlink's satellite internet communications for connectivity, military personnel orchestrated and executed precision strikes on enemy targets. Furthermore, Starlink facilitated streaming of imagery from the frontlines. This real-time reporting allowed the Ukrainian armed services to broadcast their messages and rally internal audiences to support their objectives.[102] It also hampered Russian propaganda relying on fabrication and manipulation.

5.3 Russia's cyber activities

Extrapolating previous Russian wars, including the 2008 war in Georgia, it cannot be ignored that Russia had planned a short and successful invasion of Ukraine. The cyber operations were likely meant to shape the battlefield and create the conditions for a successful military intervention. During the invasion itself, and unlike the Crimean conquest,[103] conventional kinetic means are the preferred tools of warfare. While cyberattacks can be conducive to subversion – as during the prelude to the invasion – Russia realised that cyberattacks have less strategic utility than kinetic attacks, especially in a war-like scenario.[104]

After the stalled invasion, the dedicated state-actors involved in cyber activities apparently had to restart their planning. But gathering actionable intelligence about an actual target, designing and developing cyber weapons that create

[99] Казаченко and Пако, "Digital communication tools in a public sector: Ukraine case-study of national security providing."

[100] "How a chatbot has turned Ukrainian civilians into digital resistance fighters."

[101] Alshamy et al., "Polycentric defense, Ukraine style: Explaining Ukrainian resilience against invasion, " 25.

[102] Ewing, "Integrating nonstate intelligence: Ukraine shows how it might work, " 3.

[103] Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare.*

[104] Maschmeyer, "The subversive trilemma: Why cyber operations fall short of expectations"; Wilde, "Assess Russia's cyber performance without repeating its past mistakes"; Wilde, "Cyber operations in Ukraine: Russia's unmet expectations," 2.

surgical effects is an endeavour that requires months or even years to prepare. Though some ill-prepared efforts were made targeting energy (Ukrainian power grid attack),[105] finance, or commodities these operations had an ad-hoc character and appear not to be synchronised with other instruments of power. Or, an alternative explanation, cyber preparations, if any, were simply overrun by strategic imperatives that could be answered in time physically by air and naval forces and without time-consuming digital intelligence and preparations, tailored virtual access positions and exploits.

There could be other reasons why Russia's cyber campaign seems ineffective. Russia may be reticent to execute hard-cyber operations against Ukraine as these would reveal their information position, capacities, *modus operandi*, and waste scarce 'zero-day vulnerabilities and exploits.'[106] Furthermore, destroying Ukrainian ICT infrastructure that is useful after the war, would be illogical.[107]

Though Russia has a fair amount of cyber-related agencies within the intelligence services of the state and armed forces,[108] or liaised to the state,[109] their capacity is not infinite. Apart from Ukraine, Russian cyber operators have to cover three more audiences: domestic, (other) former Soviet republics; and NATO (and EU) and its member states.[110]

5.4 Preparation and perception: A failed Russian cyber offense?

The Russian cyber operations appear to be unsuccessful. However, the effectiveness of offensive activities – in cyberspace or any other domain – largely depends on the opponent's capability to defend. Given their experiences from the past and with the support from Western allies and commercial companies, Ukraine appeared and proved well-prepared for a cyberwar. Their entire internet communication and telecom sector was considerably hardened with the result that Russian cyberattacks were noticed early and created only limited effects.

[105] Greenberg, "Russia's Sandworm hackers attempted a third blackout in Ukraine."

[106] A 'zero-day' software vulnerability is a vulnerability that is not yet known (hence, 'zero-days' known) to the creator of that software, or for which no adequate patch has yet been developed.

[107] Vynck, Zakrzewski, and Zakrzewski, "How Ukraine's internet still works despite Russian bombs, cyberattacks"; Martin, "Cyber realism in a time of war."

[108] Key Russian cyber actors include the Federal Security Service ('FSB'), the Foreign Intelligence Service ('SVR'), military cyber capabilities within Russia's General Staff (the Main Intelligence Directorate 'GRU' and the 8th Directorate). Soldatov and Borogan, "Russian cyberwarfare: Unpacking the Kremlin's capabilities," 4-5.

[109] Including private entities, both legitimate and criminal. See: Soldatov and Borogan, "Russian cyberwarfare: Unpacking the Kremlin's capabilities," 4-5.

[110] Lin, "Russian cyber operations in the invasion of Ukraine," 36-38.

Moreover, Russian cyberattacks were planned and concentrated around the invasion, probably assuming that the operation would only take days and perhaps realising that during an all-out war, cyber weapons would be of less value than kinetic weapons. Based on an analysis of cyber activities in the on-going conflict, we can argue that cyber activities, especially wipers could have had a strategic impact. However, apart from the invasion related Viasat hack and the coinciding attacks on ISPs and Telcos, the cyber operations – including wiper-attacks – largely had an ad-hoc character and were often poorly executed and most likely not synchronised with other instruments of power.

Russian cyber activities did not prevail due to prepared Ukrainian defence combined with Russian mishap. This does not mean that Russian cyber capacities may be played down.

6. Effects and consequences

In the current war in Ukraine, cyber operations gained less public attention as they were concealed by the detrimental physical war. However, once put into the spotlight, cyber operations can be seen.

While most cyber activities during the Russia-Ukraine war are mere tedious hindrances, some activities have – or could have had – an operational or even strategic impact. On the one hand, Russia's initial attacks, including on Viasat, did create a digital vacuum hampering the Ukrainian defences. Destructive wiper-attacks, such as targeted against Viasat, can have a strategic impact when they undermine the vital infrastructures of a state. The use of wipers did not come to fruition during the war so far, but their risk is still lurking.

On the other hand, soft-cyber or digital influence operations can have strategic value. While mobilising support via a single tweet may be seen a nuisance, the collective and synchronised effect of digital influence operations is of strategic importance for both sides. Pro-Russia narratives seek to demoralise Ukrainians, sow division between Ukraine and its allies and bolster perceptions of Russia. While for Ukraine, international support is both its lifeline and its Achilles' heel and thus the centre of gravity. The analysis underscores Smeets & Harknett's assessment that cyber operations can have strategic impact.[111] This not only relates to hard-cyber operations, in the Russia-Ukraine war the digital influence (soft-cyber) operations are the ones with strategic value.

The effectiveness of cyber operations still suffers from its comparison to kinetic military 'dogs of war.' Instead of using the war-peace dichotomy, cyber operations

[111] Harknett and Smeets, "Cyber campaigns and strategic outcomes," 90.

ought to be assessed on whether they have strategic, operational or tactical usage and effects away from the context in which and by whom they are used. Not least since techniques and knowledge – which comes at low costs – will proliferate to and can be used by all state and non-state actors worldwide.

The war will stop one day, but the strategic competition in cyberspace will probably prevail and NATO and EU member states are quite likely to become the next targets. Hostile and malign activities in cyberspace are not confined to a state of war and we have to realise that the cyber dogs were unleashed ages ago.

Kraesten L. Arnold

Kraesten L. Arnold M.Sc. is Assistant Professor of Cyber Operations at the NLDA and cyber operations researcher and lecturer at the NLDA. He is Lieutenant-Colonel in the Royal Netherlands Air Force and one of the founding fathers of the armed forces' Cyber Command. His academic focus lies on nation states' potential use of digital warfare.

Peter B.M.J. Pijpers

Peter B.M.J. Pijpers Ph.D. is Associate Professor of Cyber Operations at the Netherlands Defence Academy and researcher at the Amsterdam Centre for International Law (ACIL), University of Amsterdam. The main focus of his research is related to the legal and cognitive dimension of influence operations in cyberspace, below the threshold of the use of force.

Paul A.L. Ducheine

Paul A.L. Ducheine M.Sc., LL.M. is the Netherlands Defense Academy (NLDA) Professor for Cyber Operations and the co-chair of its War Studies Department. He is endowed Professor of Law for Military Cyber Operations at the University of Amsterdam and a researcher at the Amsterdam Centre for International Law (ACIL). Brigadier-General Ducheine is a Legal Advisor (Army Legal Service).

Peter Schrijver

Peter Schrijver MA is a Ph.D. researcher affiliated with the Netherlands Defense Academy. He is a Lieutenant-Colonel in the Royal Netherlands Army. His academic interests focus on Ukraine's operations in the information environment.

Bibliography

Ajir, Media, and Bethany Vailliant. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly*, 2018, 70–89.

Alshamy, Yahya et al., Polycentric Defense, Ukraine Style: Explaining Ukrainian Resilience Against Invasion. G*MU Working Paper in Economics No. 23-03,* 19 January 2023.

Baezner, Marie, and Patrice Robin. "Cyber and Information Warfare in Elections in Europe." CSS Cyber Defense Project, December 2017.

Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." *Carnegie Endowment for International Peace*, December 2022.

Beecroft, Nick. "Evaluating the International Support to Ukrainian Cyber Defense." *Carnegie Endowment for International Peace*. 'Cyber Conflict in the Russia-Ukraine War' paper series, November 3, 2022.

Black, Dan. "Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences." 2023.

Bronk, Justin, Nick Reynolds, and Jack Watling. "The Russian Air War and Ukrainian Requirements for Air Defence." *RUSI Special Report*, 7 November 2022.

Bouwmeester, Han A.J.H. *Krym Nash: An Analysis of Modern Russian Deception Warfare*. Dissertation Utrecht University 2020.

Bowen, Andrew S. "Russian Cyber Units." *Congressional Research Service*, 2022.

Clark, Brian."The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum*, 30 July 2022.

Colom-Piella, Guillem. "The Bear in the Labyrinth." *RUSI Journal* 167, no. 6/7 (2023).

"Cyber Dimensions of the Armed Conflict in Ukraine." *Cyber Peace Institute*, no. March (2023): 1–27.

Dalsjö, Robert, Jonsson, Michael, and Norberg, Johan. "A Brutal Examination: Russian Military Capability in Light of the Ukraine War." *Survival, Global Politics and Strategy* 64, no. 3 (2022): 7-28.

DCDC. "JDP 04 2nd Edition: Understanding and Decision-Making." 2016.

Ducheine, Paul A.L., Kraesten L. Arnold, and Peter B.M.J. Pijpers. "Decision-Making and Parliamentary Control for International Military Cyber Operations by The Netherlands Armed Forces." In *Military Operations and the Notion of Control Under International Law: Liber Amicorum Terry D. Gill*, edited by Rogier Bartels, Jeroen C. van den Boogaard, Paul A.L. Ducheine, Eric Pouw, and Joop E.D. Voetelink, 59–81. New York: Springer, 2020.

Ducheine, Paul A.L., Jelle van Haaster, and Richard van Harskamp. "Manoeuvring and Generating Effects in the Information Environment." In *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis – NL ARMS 2017*, edited by Paul A.L. Ducheine and Frans P.B. Osinga. The Hague: Aser Press, 2017.

Ducheine, Paul A.L., Peter B.M.J. Pijpers, and Kraesten L. Arnold, "The Next War Would Be a Cyberwar, Right?" In *Debating the Future of War (after the Invasion of Ukraine)*, edited by Jeff Michaels & Tim Sweijs (Forthcoming). See also: SSRN: https://ssrn.com/abstract=4289723 or http://dx.doi.org/10.2139/ssrn.4289723.

Ewing, Thomas. "Integrating Nonstate Intelligence: Ukraine Shows How It Might Work." *National Intelligence University, Research Short*, December 7, 2022.

EU vs Disinformation. "Weapons of Mass Delusion." 2022.

Fleming, Jeremy. "The Head of GCHQ Says Vladimir Putin Is Losing the Information War in Ukraine." *The Economist*, 2022, 2023.

Flockhart, Trine, and Elena A. Korosteleva. "War in Ukraine: Putin and the Multi-Order World." *Contemporary Security Policy* 43, no. 3 (2022): 466-81.

Galeotti, Mark. *Putin's Wars: From Chechnya to Ukraine*. Oxford: Osprey Publishing, 2022.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38, no. 2 (2013): 41-73.

Giles, Keir. "Handbook of Russian Information Warfare." *NATO Defence College* 9, November (2016): 1-90.

Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." *Wired*, (2022).

Haaster, Jelle van. "On Cyber: The Utility of Military Cyber Operations During Armed Conflict." Dissertation Amsterdam University, 2018.

Harknett, Richard J, and Max Smeets. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies*, 45(4), 2022, 534-567.

Helmus, Todd C. "The Ukrainian Army Is Leveraging Online Influences: Can the U.S. Military?" *War On The Rocks*, 1 March 2023.

Hansel, Misha. "Great Power Narratives on the Challenges of Cyber Norm Building." *Policy Design and Practice*, Vol. 6 No. 2, 2023.

Hogue, Simon. "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War." *Surveillance & Society*, Vol. 21 No. 1, 2023.

Jin, Hyunjoo. "Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet." *Reuters*, 2022.

Kazachenko, Volomymr and Arminda, Paço. "Digital Communication Tools in a Public Sector: Ukraine Case-study of National Security Providing." *Research Gate Article*, June 2 2022.

Keulen, Roy van. *Digital Force: Disrupting Life, Liberty and Livelihood in the Information* Dissertation, Leiden University, 2018.

Kleisner, Theodore W., and Trevor T Garmey. "Tactical TikTok for Great Power Competition: Applying the Lessons of Ukraine's IO Campaign to Future Large-Scale Conventional Operations." *Military Review*, April 2022.

Kostyuk, Nadiya, and Aaron Brantly. "War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation." *Contemporary Security Policy* 43, no. 3 (2022): 498-515.

Kostyuk, Nadiya, and Erik Gartzke. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 5, no. 3 (2022).

Lab, Kaspersky. "Evaluation of Cyber Activities and the Threat Landscape in Ukraine Takeaways from Kaspersky for International Discussions on Stability in Cyberspace." *Kaspersky Secure List*, May (2022).

Lam, Tong. "The People's Algorithms: Social Credits and the Rise of China's Big (Br)Other." In *The New Politics of Numbers: Utopia, Evidence and Democracy*, edited by Andrea Mennicken and Robert Salais, 71–95. New York: Palgrave MacMillan, 2022.

Lichtenstein, Dennis, Katherina Esau, Lena Pvlova, Dmitry Osipov, and Nikita Argylov. "Framing the Ukraine Crisis: A Comparison between Talk Show Debates in Russian and German Television." *The International Communication Gazette* 81, no. 1 (2019): 66-88.

Lin, Herbert S. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7, no. 4 (2022): 31-46.

Lindsay, Jon, and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In *The Power to Hurt: Coercion in Theory and in Practice*, edited by Kelly M. Greenhill and Peter J.P. Krause, 179–203. Oxford University Press, 2016.

Ling, Justin. "How U.S. Bioweapons in Ukraine Became Russia's New Big Lie." *Foreign Policy*, 10 March 2022.

Lupion, Miranda. "The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News." *Journal of Slavic Military Studies* 31, no. 3 (2018): 329-53.

Martin, Cairan. "Cyber Realism in a Time of War." *Lawfare*, 2 March 2022.

McDaid, Cathal. "The Mobile Network Battlefield in Ukraine – Part 1." *ENEA Blog*, 29 March, 2022.

Maschmeyer, Lennart. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46, no. 2 (2021): 51-90.

Mironova, Vera. "Russia's Invasion of Ukraine Is Also Being Fought in Cyberspace." *Atlantic Council*, 20 April, 2023.

Musk, Elon. "Starlink Service Is Now Active in Ukraine." *Twitter*, 26 February, 2022.

Osinga, Frans P.B. "Science, Strategy and War: The Strategic Theory of John Boyd." University of Leiden, 2005.

Pijpers, Peter B.M.J. *Influence Operations in Cyberspace: On the Applicability of Public International Law during Influence Operations in a Situation Below the Threshold of the Use of Force*. PhD Dissertation University of Amsterdam, 2021.

Pijpers, Peter B.M.J., and Kraesten L. Arnold. "Conquering the Invisible Battleground." *Atlantisch Perspectief* 44, no. 4 (2020).

Pijpers, Peter B.M.J., and Paul A.L. Ducheine. "'If You Have a Hammer': Shaping the Armed Forces' Discourse on Information Maneuver." *International Journal of Intelligence and CounterIntelligence* 36, no. 3 (2023).

Polyakova, Alina, and Spencer P Boyer. "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition the New Geopolitics." *Brookings – Robert Bosch Foundation*, no. March 2018.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

———. "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." *Select Committee on Intelligence United States Senate*. 2017.

Schulze, Matthias, and Mika Kerttunen. "Cyber Operations in Russia's War against Ukraine." *SWP Comments*, 2023.

Shires, James. *The Politics of Cybersecurity in the Middle East*. London: C Hurst & Co Publishers Ltd, 2021.

Smeets, Max. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. London: Hurst Publishers, 2022.

———. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* Fall (2018): 90–113.

Smith, Brad. "Defending Ukraine: Early Lessons from the Cyber War." *Microsoft*, 22 June 2022.

Soesanto, Stefan. "A Digital Army: Synergies on the Battlefield and the Development of Cyber- Electromagnetic Activities (CEMA)." 2021. https://doi.org/10.3929/ethz-b-000502731.

Soldatov, Andrei, and Irina Borogan. "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities." *Centre for European Policy Analysis (CEPA)*, 8 September, 2022.

Sonne, Paul, Missy Ryan, and John Hudson. "Russia Planning Potential Sabotage Operations in Ukraine, U.S. Says." *The Washington Post*, January 14, 2022.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 101-8.

Theohary, Catherine A., and John R. Hoehn. "Convergence of Cyberspace Operations and Electronic Warfare Effects." *Congressional Research Service*, no. August (2019).

Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17, no. 2 (2004): 237-56.

United Kingdom Ministry of Defence. "Multi-Domain Integration (Joint Concept Note 1/20)," 2020.

Valeriano, Brandon. "War Is Still War: Don't Listen to the Cult of Cyber." *The National Interest*, no. May (2022).

Vynck, G.D., R.L.C. Zakrzewski, and C. Zakrzewski. "How Ukraine's Internet Still Works despite Russian Bombs, Cyberattacks." *The Washington Post*, March 29, 2022.

Walton, Calder. "What's Old Is New Again: Cold War Lessons for Countering Disinformation." *Texas National Security Review* 5, no. 4 (2022).

Watling, Jack and Reynolds, Nick. "Ukraine at War: Paving the Road From Survival to Victory." *RUSI Special Report*, 4 July 2022.

Weymouth, Lally. "Volodymyr Zelensky: 'Everyone Will Lose' If Russia Invades Ukraine." *The Washington Post*, January 20, 2022.

Whyte, Christopher, and Brian Mazanec. *Understanding Cyber Warfare: Politics, Policy and Strategy*. Abingdon: Routledge, 2019.

Wilde, Gavin. "Assess Russia's Cyber Performance Without Repeating Its Past Mistakes." *War On The Rocks*, July 21, 2022.

———. "Cyber Operations in Ukraine: Russia's Unmet Expectations." *Carnegie Endowment for International Peace*, no. December (2022).

Withington, Thomas. "Russian EW: Underused or a Potemkin Capability?" *Shephard*, March 1, 2022.

Zaporozhchenko, Ruslan. "The End of 'Putin's Empire?' Ontological Problems of Russian Imperialism in the Context of the War against Ukraine, 2022." *Problems of Post-Communism*, 2023.