The 'Next' War Should Have Been Fought in Cyberspace, Right?

An Analysis of Cyber-Activities in the 2022 Russo-Ukraine War

Ducheine, P.A.L.; Pijpers, P.B.M.J.; Arnold, K.L.

DOI
10.2139/ssrn.4289723

Publication date
2022

Document Version
Final published version

University of Amsterdam

Amsterdam Center for International Law

The 'Next' War Should Have Been Fought in Cyberspace, Right? An Analysis of Cyber-Activities in the 2022 Russo-Ukraine War

Paul A.L. Ducheine

Peter B.M.J. Pijpers

Kraesten L. Arnold

Amsterdam Law School Legal Studies Research Paper No. 2022-47

Amsterdam Center for International Law No. 2022-15

The 'Next' War Should Have Been Fought in Cyberspace, Right?

An analysis of cyber-activities in the 2022 Russo-Ukraine War

Paul A.L. Ducheine, Peter B.M.J. Pijpers, & Kraesten L. Arnold [*]

Keywords: Cyberspace, Russo-Ukraine War, Hard-Cyber operations; Soft-cyber operations; Digital Influence operations; Future of War.

'Cyberwar has come'[1]

Abstract

Given the integration of Information & Communication Technology (ICT) in social interaction and in modern society at large, it is only logical that armed forces have factually developed cyber capabilities for that 'niche' kind of social interaction – warfare – too. Especially after officially embracing cyberspace as a warfighting domain, the prediction – only half a decade ago – that 'the next war will be fought in cyberspace (too)' was not an absurd idea. At first glance, the on-going 'next' war, the armed conflict between the Russian Federation and Ukraine, this assumption appears to be flawed. Or at least, the validity may be disputed. However, the question that deserves answering is whether cyber capabilities have indeed been used, and if so, what effects were sought, by whom, and against what/who. What appears obvious is that – as expected – digital influence or soft-cyber operations have been used by both fighting parties. Unexpected is the rather limited number of 'hacks' or hard-cyber operations so far that can be attributed to the warring armed forces, for which explanations will be sought. Unforeseen however, is the number of non-state hacktivist groups, such as Anonymous and the IT Army of Ukraine, that have joined the wider conflict on both sides with soft- and hard-cyber operations. Most notably, are the numerous public and commercial ICT-service providers that – in various way are actively engaged in this war and/or in the wider conflict; whether as a result of sanctions, or on moral or commercial grounds. Hence, the 'next' war was indeed conducted in cyberspace too, however, in another way as predicted, especially when looking at the wider conflict.

[*] Paul A.L. Ducheine is the Netherlands Defence Academy (NLDA) Professor for Cyber Operations and endowed Professor of Law for Military Cyber Operations and Cyber Security at the University of Amsterdam. Peter B.M.J. Pijpers is an Associate Professor of Cyber Operations at the NLDA and researcher at the Amsterdam Centre of International Law, University of Amsterdam. Kraesten L. Arnold is Assistant Professor of Cyber Operations at the NLDA and cyber operations researcher at the NLDA. Corresponding author: p.a.l.ducheine@uva.nl.

[1] Thomas Rid, "Why You Haven't Heard About the Secret Cyberwar in Ukraine," *The New York Times*, March 20, 2022.

1. Introduction

Early as 1997, John Arquilla and David Ronfeldt predicted that 'cyberwar is coming'.[2] A discourse started, culminating in the antagonising contributions by Thomas Rid stating that 'cyberwar will not take place'[3] and John Stone arguing that 'cyberwar will take place'.[4] When assessing the trains of thought the discourse was not a dichotomy of arguments, but rather an analysis based on a different perspectives - with a pinch of semantics. It did however epitomise the struggle by academics and policymakers what to make of the disruptive power of operations in or through cyberspace and how to assess, interpret or even frame these in term of international politics and law.[5]

With the Russian invasion in Ukraine in 2022 cyberwar has come! Or has it?[6] In recent decades information and communication technology (ICT) has become an integrated part, and has penetration deep in the capillaries, of our societies. Cyberspace appeared to be well suited for social interaction in general, not only for benign purposes, but also for malevolent goals such as crime, sabotage, manipulation and subversion. In recent years, numerous cyberoperations have already been executed, including the 2007 Operation Orchard,[7] the 2010 Stuxnet-attack,[8] the 2015 and 2016 Ukrainian Power outages,[9] the foreign election influence during the 2016 presidential election in the United States of America (US),[10] and NotPetya in 2017.

Modern armed forces also have embraced cyberspace as a warfighting domain and subsequently developed cyber capabilities preparing for a niche within social interaction: war and engagement in cyberspace.[11] Hence, the thought that 'the next war will be fought in cyberspace (too)' was more than imaginary.

The pitfall in the discussion whether cyberwar will or will not take place is that it is framed as a dichotomous or even binary approach. Therefore, when the Russian Federation

---

[2] John Arquilla and David Ronfeldt, "Cyberwar Is Coming," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (RAND, 1997), 79–89.

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

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

[5] See e.g. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017).

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

[7] Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* Fall (2018): 90–113.

[8] Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon*, 2015.; James Long, "Stuxnet : A Digital Staff Ride," Modern War Institute, 2019.

[9] Robert Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS Industrial Control Systems Security Blog*, 2016.; Kim Zetter, "Inside the Cunning , Unprecedented Hack of Ukraine ' s Power Grid," *Wired*, 2016.

[10] Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," vol. I and II, 2019.; Renee DiResta et al., "The Tactics and Tropes of the Internet Research Agency," *U.S. Senate Documents - Congress of the United States*, 2018, 101.; Fergus Hanson et al., "Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections," 2019.

[11] North Atlantic Treaty Organisation, "Warsaw Summit Communiqué," no. July (2016), http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

(Russia) invaded Ukraine with brute force,[12] - after which both states have been engaged in an armed conflict - the rationale behind the assumption that the next war will be a cyberwar, appeared to be flawed.

But reality is not binary. When a state uses brute military force in the land and sea domain, this does not exclude the employment of other instruments of power – whether diplomatic, legal or informational – in other domains, including cyberspace.[13] The danger is that by following a binary rationale the Russo-Ukraine War will primarily be assessed as a kinetic-military confrontation (which is understandable given the immediately noticeable effects)[14] and lessons will be learned accordingly, thus missing out on, and not being prepared for, the new developments of conflict in cyberspace.

In this article the authors will make an assessment of what sorts of cyber-activities were executed in the run-up and execution of the Russo-Ukraine War, make an analysis whether and why these appear to be underutilised and what the developments in the Russo-Ukraine War mean for the future of cyberwarfare.

In order to substantiate the analysis, the article starts (§2) with a short description of the notion of cyber-capacities and their use in a conflict-paradigm. Next, the run-up to the Russo-Ukraine War that started on 24 February 2022 will be displayed (§3). The core part of the article will be an assessment of the activities in cyberspace that were witnessed during and in the prelude to the war (§4), both the hard-cyberoperations (hacking the ICT infrastructure) and the soft-cyberoperations (influencing the audiences) from the Russian and Ukrainian side. The next section (§5) will analyse the activities witnessed in the Russo-Ukraine War set against the existing notions of cyber-capacities and paradigms. The conclusion (§6) will provide an answer to the question whether the cyber capabilities are underutilised or whether this only appears to be. Finally, the discussion will elaborate on what this can entail for the future of (cyber)warfare.

2. Cyber-capacities in a wider strategic setting

Based on the strategic culture, religion, economic might, geopolitics, geography or history states have acquired a set of national vital interests. These interests are not universal but will often include safeguarding territorial security, and political and social stability. If the vital interests of a state need to be protected or furthered, the state will activate or mobilise its instruments of power, based on a national security strategy, which include diplomacy, information, military, economy, finance or lawfare.

Instruments of power can be employed in physical domains, including the land or sea domain, but could also be used in cyberspace. Cyberspace can be exploited once state (or

[12] At the moment of writing, the Russo-Ukraine War, starting as of 24 February 2022 was still on-going.
[13] Antonius J.C. Selhorst, "Russia's Perception Warfare," *Militaire Spectator*, no. 4 (2016): 148–64.
[14] Dea Bankova et al., "Six Months of the War in Ukraine," *Reuters*, 2022.; Kateryna Clark, Mason and Stepanenko, "Russian Offensive Campaign, August 17," *ISW*, 2022.

non-state) actors have sufficient offensive and defensive capabilities,[15] ranging from strategic to tactical level. Employment of cyber-capacities at the strategic level, such as foreign election interference or the process of disrupting a nuclear enrichment facility, has nation-wide impact but such bespoke operations will take years to prepare. The more tactical capabilities (obtaining an electromagnetic footprint of a person or spear-phishing a social media community) can be executed via 'off-the-shelf' products.

A strategy can be employed in different (or in a multitude of) circumstances; war, peace, domestic or abroad. States will have different authorities, agents and legal frameworks – taken together as security paradigms[16] - to cope with these different circumstances. To defend against malign actors who conduct (cyber)crime activities the state requires law enforcement capabilities; the prevention of damage to, and protection and restoration of ICT hardware, software and data requires (national) cyber security; insight and foresight in digital threats requires an intelligence gathering capability and subsequent legal framework; and finally, during an armed conflict states need to be able to create effects with cyber-capabilities and must be capable of preventing or countering similar malicious effects.

Cyber strategies, unleashing offensive, defensive or deceptive capacities[17] entail three sorts of operations. First, digital intelligence operations – or cyber espionage[18] – obtain, steal or reproduce data and information without manipulating or destroying them.[19]

Second, digital undermining or hard-cyberoperations are activities in cyberspace targeting and creating effects on the very components of cyberspace. Figuratively speaking, malicious software (malware) and data are the 'weapons' or 'payloads' used. Examples include attacks on the availability, confidentiality or integrity of virtual identities (social media accounts, websites), virtual objects (computer programs, software, data) or hardware (servers, routers). These days many physical objects and systems depend on faultless operating computers and networks, subsequent effects of cyberoperations may materialise beyond cyberspace and thus affect the functioning of other physical objects such as (civilian) critical infrastructures or military (weapon) systems.

Finally, unlike hard-cyberattacks that target (the objects in) cyberspace itself, soft-cyberattacks or digital influence operations merely use (or abuse) cyberspace as a 'vector' to influence the psyche of targeted audiences, such as 'cyber-enabled' psychological warfare,

[15] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," 2018.; Public Affairs Office, "U.S. Conducts First Hunt Forward Operation in Lithuania," *US Cyber Command*, 2022.

[16] Paul A.L. Ducheine and Peter B.M.J. Pijpers, "The Notion of Cyber Operations," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021).

[17] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

[18] Russell Buchan and Inaki Navarrete, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021), 231–52.

[19] These cyber related intelligence operations are not the focus of this research. From more information on this see part 1 & 2 of Neveen Shaaban Abdalla et al., "Intelligence and the War in Ukraine," *War On The Rocks*, 2022.

propaganda or information operations.[20] In a figurative sense, information is then used as 'weapon'. In practice, hard- and soft-cyberattacks often complement each other. Consider, for example, a phishing mail to lure individuals into revealing login credentials, after which an attacker may manipulate, destroy or steal data. Next, sensitive or undisclosed information may be revealed (hack-and-leak) to cause a commotion.

3. The conflict between Russia and Ukraine

The Russian Federation – and its predecessors – and Ukraine, with its capital Kiev, have always had a special relation, one that is crucial in the post-Soviet foreign policy that is centred on the notion to reinstall the great Russian empire.[21] Ever since the rise of Vladimir Putin as the main actor in the Russian government a policy of spheres of influence around Russia has been pursued, implying that states including Belarus, Georgia and Ukraine should be a geographical, political and cultural buffer zone between Russia and the West. So-called compatriots (Russian speakers in former Soviet states who identify themselves as ethnically Russian)[22] constitute one of the tentacles of that policy. Avoiding a hard-power confrontation with these former Soviet states – with the debacle of the 1994/1995 Chechnya war in mind – Russia started to experiment with the application of soft-power[23] or more hybrid forms of exerting power.[24] The emergence of cyberspace and with it the Internet and social media provide ample impetus to 'weaponize digital media'[25] – i.e. to frame information on social media and use the narration as an instrument of soft power in political warfare - in gaining domestic and international support and to persuade compatriots to turn away from Western culture and ideology.

Ukraine has been subjected to Russian influence for a long time, starting with the interference in the 2004 elections. The ensuing Orange revolution in response, marked the Ukrainian desire to affiliate with the EU and possibly NATO rather than Russia, hence revolting against Russian policy.

---

[20] Cyber operations make use of the electromagnetic spectrum, the latter can also be used as a 'stand-alone' or supplementary capability to generate effects in electronic warfare. Electronic warfare (EW) makes use of energy while cyberspace operations use a binary code and are often internet based. Both aspects can be combined if a malign virus (binary software) is send via an EW asset e.g. during the 2007 Operation Orchard. See: Stone, "Cyber War Will Take Place!" pp. 16-17.

[21] Holger Möldera and Vladimir Sazonovb, "Information Warfare as the Hobbesian Concept of Modern Times — the Principles, Techniques, and Tools of Russian Information Operations in the Donbass," *Journal of Slavic Military Studies* 31, no. 3 (2018): 308–28. pp. 315-319; Clint Reach, "The Origins of Russian Conduct," *Prism* 9, no. 3 (2022). pp. 7-9.

[22] Miranda Lupion, "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. p. 330.

[23] Joseph S. Nye Jr., "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71. For example the policy of 'passportisation', see: James A Green, Christian Henderson, and Tom Ruys, "Russia's Attack on Ukraine and the Jus Ad Bellum," *Journal on the Use of Force and International Law*, 2022. p. 13.

[24] James Rodgers and Alexander Lanoszka, "Russia's Rising Military and Communication Power: From Chechnya to Crimea," *Media, War & Conflict*, 2021.; Möldera and Sazonovb, "Information Warfare as the Hobbesian Concept of Modern Times — the Principles, Techniques, and Tools of Russian Information Operations in the Donbass." pp 319-322.

[25] Lupion, "The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News."

Tensions culminated when, in the early months of 2014, Russia invaded and subsequently annexed the Crimean Peninsula cutting short Ukrainian aspirations.[26] Pro-Russian armed separatists simultaneously took control of parts of the Donbas area in Eastern Ukraine. Aside from fairly straightforward Distributed-Denial-of-Service (DDoS) attacks, these kinetic operations were not accompanied with sophisticated cyberattacks.[27]

After the annexation, Russia used numerous information tools to influence and tighten the grip on the Donbas' and wider Ukrainian population.[28] Historical myths, narratives and symbols – including the Kremlin's 'demilitarization and denazification' narrative - were used via a deluging plethora of media outlets to disorient the targeted audiences,[29] amongst others during Ukraine's May 2014 presidential election. Apart from digital influence operations, pro-Russian hacker group 'CyberBerkut' had compromised Ukraine's Central Election Commission's vote-counting software that would designate ultra-right leader Yarosh as winner of the elections, regardless of the actual votes cast. Right after the elections, the very same manipulated results were presented on Russian TV channel 1. However, the hack was discovered just in time and the malicious software was sanitised at the very last moment. The result was that the pro-Western politician Poroshenko was elected president with an absolute majority.[30]

The years thereafter, a long chain of Russian-attributed needle-prick cyberattacks targeted a variety of Ukrainian government organisations, critical infrastructures and corporate businesses.[31] In 2015, hackers attacked Ukraine's power grid, causing a power outage in parts of the country. A year later, Ukraine's electricity distribution system was again targeted. The cyberattacks did not only temporarily deny service of these Industrial Control Systems (ICS), the victim's computer monitoring systems also were deliberately corrupted, rendering them inoperable. The Security Service of Ukraine (SBU) attributed both attacks to the Russian state or state-sponsored hackers. Later, cyber security firm Kaspersky Lab substantiated that accusation.[32] In retrospect, since 2014, Ukraine appeared to be a testing ground for refining Russian hard-cyberattacks on critical infrastructure.[33]

---

[26] Peter B.M.J. Pijpers and Eric H. Pouw, "Sovereignty in Cyberspace : Lessons from the Ukrainian Case," *Atlantisch Perspectief* 46, no. 3 (2022): 36–41.; Han A.J.H. Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare*, 2020.

[27] M. C. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks," 2020 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 199-213.

[28] Brendan Chrzanowski, "An Episode of Existential Uncertainty: The Ontological Security Origins of the War in the Donbas," *Texas National Security Review* 4, no. 3 (2021): 11–32.

[29] Möldera and Sazonovb, "Information Warfare as the Hobbesian Concept of Modern Times — the Principles, Techniques, and Tools of Russian Information Operations in the Donbass." pp 322-325.

[30] David E. Sanger, *The Perfect Weapon : War, Sabotage, and Fear in the Cyber Age* ([S.l.]: Scribe, 2018). pp. 90-98.

[31] Lee, Assante, and Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid."

[32] Kaspersky Lab, "Newly Discovered BlackEnergy Spear-Phishing Campaign Targets Ukrainian Entities," Kaspersky, 2016.

[33] Sanger, *The Perfect Weapon : War, Sabotage, and Fear in the Cyber Age*. Chapter VII (Putin's Petri Dish) p. 90; Kim Zetter, "The Ukrainian Power Grid Was Hacked Again," Motherboard, 2017.

One hard-cyberattack particularly aimed at a (military) weapon system concerns malware implanted on Android devices via the Russian social media platform *VKontakte* by Russian Military Intelligence (GRU) hackers. The original application enabled Ukrainian artillery forces to more rapidly process targeting data of their Soviet-era artillery units. From late 2014 to 2016, the manipulated application was able to retrieve communications and some locational data from infected devices. That intelligence was used to strike against Ukrainian artillery units operating against pro-Russian separatists in Eastern Ukraine, resulting in an estimated fifteen to twenty percent loss of their pre-war 'D-30' howitzer arsenal in combat operations.[34]

Of the pre-2022 cyberattacks, the 2017 'NotPetya' cyberattack – executed on the eve of Ukraine's Constitution Day commemorating the country's exit from the Soviet Union – was perhaps the most devastating.[35] Initially meant to target Ukraine's fiscal system, the malware soon spread and infected businesses and critical infrastructures worldwide, resulting in a collective loss of nearly $1 billion.[36]

In concert, soft-cyberattacks were executed targeting both Ukrainian and Western audiences. A cyber-enabled influencing operation can be found in the aftermath of the crashing of Malaysia Airlines Flight MH-17 in July 2014, while flying over eastern Ukraine near the Ukrainian/Russian border. The international investigation team concluded that the aircraft had been shot down by a 'Buk' surface-to-air missile system. Russian involvement in the provision of the missile system was demonstrated, but the Russian Government denied all responsibility and kept providing a variety of alternative possibilities for the crash via social media platforms, web fora and online news sites. The investigation team considered, analysed and subsequently excluded other possibilities based on the evidence available.[37]

Moreover, both Russia and Ukraine have framed the conflict via mainstream and social media which in turn enhances the construction of different and often mutually exclusive views on the conflict in Eastern Ukraine among pro-Ukrainian and pro-Russian communities,[38] resulting in increased polarisation.

Late 2021, the tensions raised again when Russia was building up forces along the Ukrainian border for the quadrennial military exercise Zapad (the West). In December, in response to Western concerns, Russia issued a list of security guarantees the West and especially NATO should provide to ease tensions. Russia blamed NATO of discarding the post-Cold

[34] Crowdstrike Global Intelligence Team, *Use of Fancy Bear Android Malware in tracking of Ukrainian Field Artillery Units*, December 22, 2016, updated March 23, 2017.
[35] Alina Polyakova 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). p. 14.
[36] US Department of Justice, "The NotPetya Cyber Attacks", United States district court western district of Pennsylvania, Indictment No. 20-316, October 15, 2020, pp. 16–23.
[37] Dutch Safety Board, Crash of Malaysia Airlines flight MH17, Hrabove, Ukraine, 17 July 2014 (Report), p 253.
[38] M. Makhortykh and M. Sydorova, "Social Media and Visual Framing of the Conflict in Eastern Ukraine," *Media, War and Conflict* 10, no. 3 (2017): 359–81. pp. 375-377.

War agreement since NATO had expanded to the East and renounced long-standing weapon treaties.[39] Russian officials stated that ignoring the Russian interests could 'lead to a "military response" similar to the Cuban missile crisis of 1962'.[40]

4. An overview of cyber-activities in the Russo-Ukraine War

The Russian policy to use soft and hybrid powers to exert influence, combined with the Russian information- and cyber-related activities inside and outside of the Russian sphere of influence (none of which surpassed the threshold of the use of force, as laid down in Article 2(4) of the UN Charter)[41] was inducive to the assumption that Russian military and informational instrument of power would go in tandem.[42] Stronger still, it was expected that Russian influence operations would revolve around the application of activities in cyberspace, thereby sabotaging and undermining activities targeting critical infrastructure as well as influencing the cognition of target audiences.[43]

Since cyberoperations were expected, the military invasion came as a surprise. Moreover, the military employment of kinetic force overwhelmed other instruments of power provoking many to argue that cyber-activities were non-existent, or that these were hardly effective. Before analysing these claims, it is pivotal to assess what activities in cyberspace did take place.

4.1. The prelude to the 2022 Russo-Ukraine War

In January and February 2022, the two months preceding the actual invasion, pro-Russian hackers executed various cyberattacks. These attacks started with rather straightforward denial-of-service attacks on online service providers, their servers and network equipment, the Ukrainian Ministry of Defence, the Armed Forces and two national banks.[44] Almost simultaneously, pro-Russian hackers defaced the websites of dozens of government organisations, after which they showed manipulated political imagery and provocative statements.[45] Spear-phishing mails supposedly originating from Ukrainian state bodies and targeting Ukrainian entities supplement the range of cyberattacks with only 'modest impact'. Noteworthy is that Belarusian 'Cyber Partisans' hacked their country's railway

[39] "Putin Blames West for Tensions as Fears Rise over Ukraine," *Al Jazeera*, December 21, 2021.
[40] Andrew Roth, "Russia Issues List of Demands It Says Must Be Met to Lower Tensions in Europe," *The Guardian*, December 17, 2021.
[41] United Nations, "Charter of the United Nations" (1945).
[42] Rodgers and Lanoszka, "Russia's Rising Military and Communication Power: From Chechnya to Crimea." p. 2.
[43] In Russian policies – which less frequently use the word 'cyber' - these are coined the information-technology warfare and information-psychological warfare. Keir Giles, "Handbook of Russian Information Warfare," *NATO Defence College* 9, no. November (2016): 1–90. pp 8-10
[44] Ukrainian Centre for Strategic Communication, 15 February 2022, https://spravdi.gov.ua/uvaga-zhodnoyi-zagrozy-dlya-koshtiv-vkladnykiv-pryvatbanku-nemaye/
[45] Security Service of Ukraine, Cyber Attacks on Government Websites, 14 January 2022, , https://ssu.gov.ua/en/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv, Accessed September 7, 2022

network to disrupt the transport of Russian troops to Ukraine.[46] Mid-January 2022, Microsoft revealed the existence of a destructive malware operation (dubbed '*WhisperGate*') targeting multiple organisations in Ukraine.[47] This destructive 'wiperware'-attack, attributed to the Russian Military Intelligence Service (GRU),[48] had been designed to inflict permanent damage. Masquerading as mere 'ransomware', this malware not only hijacked data, but also erased data on attacked computers intending to render these computers useless.

Already in the prelude to the war, Ukraine increased its resilience to counter the Russia cyberattacks,[49] cognisant of an upcoming war in cyberspace or even in the physical realm. On invitation, US Cybercommand supported Ukraine for three months as of December 2021.[50]

On February 23, 2022, still one day prior to the invasion, several cybersecurity firms sounded the alarm since they had found other malicious software, again with destructive 'disk-wiping' capabilities, targeting hundreds of machines in Ukraine in the financial, defence, aviation, and IT services sectors.[51] This newly discovered '*HermeticWiper*' malware showed some similarities with the earlier discovered wiperware, but in a more sophisticated guise.

On the eve of the invasion, on February 24, one particular occurrence attracted the attention: the cyberattack on Viasat, a major satellite communications provider for Ukraine and its military but also for large parts of Europe. The allegedly Russian cyberattack rendered satellite modems unserviceable and had immediate and severe effects on the Ukrainian military's battlefield communications, particularly in the Chernihiv region (close to the threatened Kiev). The loss of satellite Internet communications severely hampered frontline communications and made Ukrainian forces virtually blind to Russian troops positions and movements.[52] The impact was not restricted to Ukraine, impairing Viasat also affected communication systems in other parts of Europe and Northern Africa.[53] However, after a Tweet by Ukraine's minister for Digital Transformation Fedorov to Elon Musk,[54]

---

[46] AC Vicens, "Details emerge on hack of Belarusian Railways and the group behind it", Cyberscoop, January 26, 2022; Peter Dickinson, "Cyber Partisans Target Russian Army in Belarus amid Ukraine War Fears," *Atlantic Council*, 2022.

[47] Microsoft Threat Intelligence Centre (MSTIC), Destructive malware targeting Ukrainian organizations, 15 January 2022.

[48] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, June 22, 2022.

[49] Lally Weymouth, "Volodymyr Zelensky : ' Everyone Will Lose ' If Russia Invades Ukraine," *The Washington Post*, January 20, 2022.; Paul Sonne, Missy Ryan, and Hudson. John, "Russia Planning Potential Sabotage Operations in Ukraine , U . S . Says," *The Washington Post*, January 14, 2022.

[50] Alexander Martin, "US Military Hackers Conducting Offensive Operations in Support of Ukraine , Says Head of Cyber Command," *Sky News*, 2022.

[51] Symantec Threat Hunter Team, Ukraine: Disk-wiping Attacks precede Russian Invasion, 24 February 2022,

[52] Jason Blessing, American Enterprise Institute, Revisiting the Russian Viasat Hack: Four Lessons About Cyber on the Battlefield, September 02, 2022.

[53] "Satellite Outage Knocks out Thousands of Enercon's Wind Turbines," *Reuters*, February 28, 2022.

[54] Elon Musk, "'Starlink Service Is Now Active in Ukraine,'" *Twitter*, 2022, https://twitter.com/elonmusk/status/1497701484003213317?s=11.

the latter's Starlink satellite system – with end-to-end-encryption, was operational within hours restoring the disrupted Ukrainian Internet.[55]

4.2. The Russo-Ukraine war since 24 February 2022

Since the day of the military invasion, also non-state actors were engaged in the conflict,[56] often clearly choosing sides. That night, the notorious hacker group *Anonymous* declared a cyber war against the Russian Government.[57] Various other smaller and larger hacker groups sided with Ukraine and launched attacks on Russian targets in an effort to disrupt their invasion. The attacks were often limited to relatively harmless denial-of-service attacks and website defacements. Alleged claims of hacked Russian government institutions or other objects are often difficult to verify and value.[58]

Already on the first day of the invasion, Fedorov - using social media platforms Telegram, Facebook and Twitter - called on tech-savvy volunteers worldwide to join the newly established 'IT-Army of Ukraine' to protect his country from Russian digital attacks.[59] Albeit the IT-Army executed offensive cyberoperations, i.e. denial-of-service attacks against Russian government and company websites,[60] they are also used by the Ukrainian government as a symbol of Ukrainian cyber-resilience and perseverance.

The IT-Army goes beyond a random group of worldwide sympathizers and is mixed with an in-house expertise from the Ukrainian defence and intelligence services. This mixed group thus runs the risk to cross boundaries of legal frameworks regarding norms and rules for state behaviour in cyberspace that in turn may wreak havoc on the future stability of cyberspace. According to Soesanto, the IT-Army is "a hybrid construct that is neither civilian nor military, neither public nor private, neither local nor international, and neither lawful nor unlawful."[61]

It is fair to say that not all 'cyber patriots' sided with Ukraine. Several larger and smaller hacker groups chose to fight for the aggressor, of whom 'Sandworm', 'Conti', 'Stormous' and 'UNC1151' are some formidable adversaries.[62]

---

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

[56] Stephan Sestanovich, Thomas Graham, and Charles A. Kupchan, "Conflict in Ukraine," *Council on Foreign Relations*, 2022.

[57] https://twitter.com/YourAnonOne/status/1496965766435926039

[58] Emma Vail, The Recorded Future, The Record, Russia or Ukraine: Hacking groups take sides, February 25, 2022, updated March 3, 2022,

[59] https://twitter.com/FedorovMykhailo/status/1497642156076511233

[60] Stefan Soesanto, The IT Army of Ukraine: Structure, Tasking, and Ecosystem, Cyberdefense report, Center for Security Studies (CSS), ETH Zürich, June 2022, p. 28. Initially the IT Army appeared to be government-controlled, but closer research alluded to an affiliation with the Anonymous group.

[61] Stefan Soesanto, The IT Army of Ukraine: Structure, Tasking, and Ecosystem, Cyberdefense report, Center for Security Studies (CSS), ETH Zürich, June 2022, p. 4.

[62] Emma Vail, The Recorded Future, The Record, Russia or Ukraine: Hacking groups take sides, February 25, 2022, updated March 3, 2022; Peter B.M.J. Pijpers, "Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War," *Hybrid CoE*, no. October (2022). pp. 8-9.

In June 2022, Microsoft published a report on their lessons from the first four months of the 'cyberwar' between Russia and Ukraine.[63] Although the document was likely written from a commercial perspective, the report provides insight from a first line of cyber-defence. The company saw that Russia launched multiple waves of sophisticated destructive cyberattacks against dozens distinct Ukrainian agencies and enterprises, eventually destroying thousands of computers. Microsoft concluded that these cyberattacks were conducted largely in concert with kinetic operations.[64] Microsoft was not the only ICT actor involved in the war. After the Russian invasion, Vodafone cut communication in large parts of the Donbas region leaving the Russian separatist digitally blind.[65]

As the first Russian troops crossed the Ukrainian border, cyber security company ESET discovered two more destructive wiperware families (*HermeticWiper, IsaacWiper*) targeting Ukrainian organizations.[66] That day, also Symantec revealed yet another form of disk-wiping malware (*Trojan.Killdisk*) launched shortly before the Russian invasion, against targets in the Ukrainian financial, defence, aviation, and IT services sector.[67]

In March 2022, Ukraine's railways and transportation systems transferred weapon systems and military supplies from Western allies to the east, while large numbers of internally displaced persons and refugees used the same means to flee in the opposite direction. The very same railways and transportation systems were targeted with a variety of weapons. Destructive cyberattacks on, for example, a key logistical centre for the movement of military and humanitarian aid in Lviv were executed in concert with missile attacks on railway substations.[68]

In April, ESET reported a hard-cyberattack with so-called '*Industroyer2*' ICS-malware on the Ukrainian power grid. The attacker had modified pieces of malware that had been used earlier (*Industroyer*), in 2016, to attack the power grid and cause power outages. This time, the ICS-malware was accompanied by yet other sets of destructive wiper malware.[69]

On June 30, Ukraine's 'State Service of Special Communications and Information Protection' reported that since the invasion, Russia had launched some 800 cyberattacks, mainly targeting government and local authorities, security and defence, and the financial, energy, transport and telecom sectors. Over time, the intensity of cyberattacks had not decreased, yet their quality has been declining.[70]

---

[63] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, June 22, 2022.
[64] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, June 22, 2022, p 3.
[65] Cathal McDaid and Rowland Corr, "The Mobile Network Battlefield in Ukraine - Part 3," *Adaptive Mobile Security*, 2022.
[66] ESET Research, Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper, 01 Mar 2022,
[67] Symantec Threat Hunter Team, Ukraine: Disk-wiping Attacks Precede Russian Invasion, 24 Feb, 2022,
[68] Brad Smith, "Defending Ukraine : Early Lessons from the Cyber War," *Microsoft*, 2022. p. 8.
[69] ESET Research, Industroyer2: Industroyer reloaded, 12 Apr 2022,
[70] https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak., Accessed September 8, 2022.

Next to the aforementioned hard-cyberattacks, pro-Russian state and non-state actors conducted foreign cyber-enabled influence operations - disruptive propaganda, misinformation and disinformation campaigns (both mainstream and social media) to influence target audiences.[71] Not surprisingly, since Russia's Defence Minister Shoigu stated in 2015 that, "The day has come when we all have to admit that words, cameras, photos, the Internet and information in general have become another weapon, another component of the armed forces. This weapon can be used for good and for evil. It is a weapon that has played a role in various events in our country's history, in our defeats as well as in our victories."[72]

The use of modern digital technologies and the Internet resulted in a broader geographic reach. Influencing messages were sent to more precisely targeted audiences, with higher volumes and greater speed and agility. These soft-cyberattacks were not conducted in isolation but appeared to be linked to other (cyber) activities. False narratives were prepared to be distributed via government-managed and influenced websites, amplifying other narratives spread though exploited social media services.[73] Of note, Russia does not only target the Ukrainian government or former Soviet states in general, but also domestic Russian audiences and Western audiences.

In Russia, the TV is the most used mainstream media outlet; domestic audiences are influenced via talk shows, news reports and educational programs. Not to say that social media channels, including *VKontakte* and *Telegram*, are extensively used to disseminate framed images, memes or even Deepfakes.[74] The main purpose of Russian influence operations is to demoralise the Ukrainian population, to drive a wedge between Ukraine and its Western allies, and to augment the domestic and foreign audiences of Russia. Narratives used in this context are the fear of Russophobia, a sensitive topic to Russian diaspora or ethnic Russians living in Ukraine, the 'denazification and demilitarisation' of the Ukraine – narratives that were also used to prevent a resurgent Germany after World War II,[75] or the endemic corruption within the Ukrainian government.[76] The integrity of Western states is undermined by a report on bioweapons made in Ukraine, alluding the

[71] Theodore W. Kleisner 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*, no. April (2022). pp. 12-14.

[72] Peeter Tali, Deputy Director of the NATO Strategic Communications Centre, "Russian General Staff has already lost the information war", 16 June 2022.

[73] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, June 22, 2022, p 4.

[74] Alden Wahlstrom et al., "The IO Offensive : Information Operations Surrounding the Russian Invasion of Ukraine," *Mandiant*, 2022.

[75] Marco Longobardo, "Legal Perspectives on the Role of the Notion of « Denazification » in the Russian Invasion of Ukraine under Jus Contra Bellum and Jus in Bello," *Revue Belge de Droit International*, 2022. Para II.

[76] Dennis Lichtenstein et al., "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.

hypocrisy of the West.[77] A hypocrisy that is underlined by homophobic tropes, suggesting that Western decadence has also infected Ukraine.[78]

Ukraine's President Zelensky also fully utilizes the potential of the social media. He is addressing his own population online and keeping up the morale of his troops. Impassioned speeches to foreign parliaments, given on-screen via the Internet, resulted in the very needed diplomatic support but moreover in the supplying funds, military systems and ammunition. As an actor Zelensky already had a solid experience with social media as a means to convey particular messages to people. As president of a country under siege he benefits from these same simple platforms; followed not only by the Ukrainian population, but also people across the globe. Since the first day of this current war, social media has helped him to internationalize Ukraine's cause and to persuade (Western) democratic countries to support his country. Zelensky's quote "I need ammunition, not a ride",[79] after he had been offered transportation to safer areas, went viral. Zelensky thus recognizes the importance and influence of social media. Zelensky's use of social media boosts moral affecting the cognitive dimension of both friend and foe.

Civilians and soldiers alike used social media to show the online world the actual situation on the ground. Russian troop locations, strengths and movements are constantly being reported online, whilst such information about Ukrainian positions is carefully kept from the Internet. Official social media platforms mobilize the population and share information and instructions for non-violent and armed resistance; varying from passing information on Russian weapons and troop movements, to instructions how to attack enemy forces with Molotov cocktails.

On social media the story of a Ukrainian fighter pilot with the nickname 'the Ghost of Kyiv' became very popular. The pilot allegedly had shot down six Russian aircraft on the first day of the invasion. The identity of the pilot could not be confirmed, but a heroic legend was born. Later, the Air Force Command of the Ukrainian Forces admitted that the Ghost of Kyiv did not exist in reality, at the same time warning "not to neglect the basic rules of information hygiene, …[and]…, to check the sources of information before disseminating it."[80]

Another occurrence concerned the bold response of Ukrainian troops defending Zmiinyi Island ('Snake Island') after Russia's Black Sea Fleet flagship 'The Moskva' demanded their surrender. The explicit refusal 'Russian warship, go home'[81] became a popular phrase online

[77] Justin Ling, "How U.S. Bioweapons in Ukraine Became Russia's New Big Lie," *Foreign Policy*, 2022.; EU vs Disinformation, "Weapons of Mass Delusion," 2022.
[78] "Another Shade of Hate," *EU vs Disinformation*, 2022.
[79] Dalia Al-Aqidi, "How Zelensky Used Social Media to His Advantage," *Center for Security Policy*, 2022.
[80] Air Force Command of the Ukrainian Forces, 30 April 2022, from: https://www.facebook.com/kpszsu/posts/363834939117794
[81] The actual phrase was (translated into English) "go f**k yourself", see: https://www.theguardian.com/world/video/2022/feb/25/go-fuck-yourself-ukrainian-soldiers-snake-island-russian-ship-before-being-killed-audio

and was frequently used in internet memes; and so was the subsequently introduced postage stamp to honour the heroes. On 13 April 2022, Ukrainian officials reported that the Moskva had been hit by two Ukrainian-made anti-ship missiles.[82] A day later, Russia announced that the Moskva had sunk.[83] The Moskva's sinking was used as theme for another postage stamp and new online memes. The narrative of failing Russian activities has been amplified by online videos of Ukrainian farmers towing away abandoned Russian combat vehicles.

In March, the Ukrainian Security Service announced that it had discovered and shut down automated networks of computers ('botnets') mimicking over 100,000 social media accounts spreading disinformation to create panic among the Ukrainian population and to destabilize the socio-political situation in the country.[84]

The Internet and social media provide for swift distribution of information with a global reach; be it real, changed or entirely fake information. One may assume that Moscow thought it was well-prepared to start influence activities parallel to a kinetic ground war on Ukrainian territory. Nevertheless, Russia's efforts were less successful than anticipated. Moreover, it appeared that Ukraine is exploiting these online media capabilities best. From showing the heroics of their own soldiers and the determination of their people, to disclosing war crimes of Russian fighters, revealing the mismanagement of Russian troops, and the showing poor equipment and destroyed Russian weapons systems.

5. Analysing the Differences in Cyber-capacities used

The first observation is that the Russo-Ukraine War is not the expected fully fletched cyberwar,[85] but neither is the war not void from cyberoperations. There are and have been numerous cyberattacks in the prelude to the Russo-Ukraine War and during the armed conflict but the cyberoperations were different from what was to be expected, both in number and appearances.

5.1. What are the differences?

Cyberoperations have played a smaller role than expected. Especially hard-cyber or digital sabotage operations directed against the critical infrastructure were sparsely witnessed. Though some hard-cyberoperations were executed in the prelude to the war, they are (so far) almost absent during the war while Russia had executed numerous of these operations

[82] Digital Forensic Research Lab, "Russian War Report: Competing Narratives about the Sinking of Russia's Moskva Warship," *Atlantic Council* (blog), April 15, 2022.
[83] Jenny Hill, "Russian Warship: Moskva Sinks in Black Sea," *BBC News*, April 15, 2022.
[84] https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv, accessed September 8, 2022.
[85] In fact, the war came unexpected to many and its intensity did certainly not follow logically from the history of cyber operations during the Russo-Ukraine conflict.

in the years before the war.[86] In that sense, the dogs of war have failed to bark loudly yet.[87] Conversely, influence operations making use of the Internet and social media have been significant, as was to be expected. While the number of attacks differ from what was expected, in both hard- and soft-cyberoperations no new forms of operations were witnessed. Often, existing techniques were reused, e.g. hack-and-leak operations against Russian organisations by actors such as Anonymous, the malware-attack by APT Sandworm against the Ukrainian power grid,[88] or the Deepfakes of president Zelensky[89] and Putin.[90]

During the war, not only military targets were hit with cyberattacks. Hard-cyberoperations also targeted civilian critical infrastructure, media and financial systems. The starkest difference, however, revolves around the actors involved in the war. The cyberoperations, in the prelude to and especially during the war, have not solely been executed by the Russian and Ukrainian forces. Most prominent is the unexpected involvement of independent non-state actors,[91] on both sides.[92] One sort of non-state sympathisers are hacktivist groups such as (pro-Ukrainian) Anonymous,[93] and the pro-Russian Stormous and the Conti group that have joined the warring parties and independently targeted infrastructure or audiences.[94] The actual impact of their involvement remains a matter of further research.[95] A second set of non-state involvement are the commercial parties especially ICT-related firms including Microsoft,[96] Vodafone,[97] Facebook and Twitter,[98] and Starlink.[99] Entities that have mainly sided with Ukraine.[100]

---

[86] Niels Nagelhus Schia, "The Digital Battlefield," *Prio Bolgs*, 2022, https://blogs.prio.org/2022/03/the-digital-battlefield/.

[87] Jelena Vicic and Rupal N. Netha, "Why Russian Cyber Dogs Have Mostly Failed to Bark," *War On The Rocks*, 2022.; Nadiya Kostyuk 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).

[88] Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, 2022.

[89] Bobby Allyn, "Deepfake Video of Zelenskyy Could Be 'tip of the Iceberg' in Info War, Experts Warn," *Npr*, 2022.

[90] Stephanie Burnett, "Fact check: The deepfakes in the disinformation war between Russia and Ukraine", DW.com, 18 March 2022.

[91] Contrary to the more common involvement of proxy actors such as APTs or Glavsent (Internet Research Agency).

[92] Emma Vail, "Russia or Ukraine : Hacking Groups Take Sides," *The Record*, 2022.

[93] Anonymous, "We Call All Hackers and Digital Activists to Be United as One. If This War Is Not Won with Weapons, It Will Be Won with Cyberweapons. Democracy and Freedom Will Destroy Fascism and Imperialism," *Twitter*, no. February (n.d.), https://twitter.com/YourAnonTeam/status/1497678548764696585.

[94] Dan Milmo, "Anonymous : The Hacker Collective That Has Declared Cyberwar on Russia," *BBC News*, 2022. "Stormous: The Pro-Russian, Clout Hungry Ransomware Gang Targets the US and Ukraine," Trustware SpiderLabs, 2022.

[95] Anh V. Vu et al., "Getting Bored of Cyberwar: Exploring the Role of the Cybercrime Underground in the Russia-Ukraine Conflict," *Arxiv*, 2022.

[96] Tom Burt, "The Hybrid War in Ukraine," *Microsoft*, 2022.

[97] McDaid and Corr, "The Mobile Network Battlefield in Ukraine - Part 3."

[98] Burt, "The Hybrid War in Ukraine." Morgan Meaker, "Russia Blocks Facebook and Twitter in a Propaganda Standoff", *Wired*, 4 March 2022.

[99] Musk, "'Starlink Service Is Now Active in Ukraine.'"; Jin, "Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet."

[100] David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *The New York Times*, 2022.

5.2. What could the reasons for the difference be? (analysis)

The role of cyberoperations in the Russo-Ukraine War differs from what was to be expected; challenging our existing knowledge. While hard-cyberoperations were sparse, soft-cyberoperations are not only numerous but they have gained significance as a means to influence. Moreover, numerous hacktivists and commercial actors have engaged in the wider conflict, not necessarily waging war, for a variety of reasons – financially-driven or idealistic purposes, forced by EU sanctions or simply to agitate.

Some cyberoperations are visible, but the question is why there's not more? When parsing the evidence as depicted in the previous sections two overall categories can be made: there are attacks, but they are not uncovered, or the number of attacks is limited – either intentional or because it all went pear-shaped.

5.2.1. There are attacks, but we do not see them.

Both Russia and Ukraine might have executed hard-cyberoperations targeting critical infrastructure of the opponent. One of the reasons attacks are not noticed (especially the Russian) is that the Ukrainian cyber defence is well organised,[101] and attacks were intercepted.[102] Over the years,[103] Ukrainian cyber infrastructure has been hardened with state (US, UK) and commercial (Microsoft) support cushioning the impact of an attack – though this coordinated defence should not be overrated.[104] Moreover, ongoing cyberattacks since the annexation of Crimea have given away in advance Russia's *modus operandi* and preferred targets.

Ukraine might withhold information. Attacks may have affected targets, but impact has not been made public, thereby hindering the opponent to make a battle damage assessment or avoiding disheartening own forces. Another possibility is that hard-cyberattacks definitely took place and caused damage but were not recognised as such.[105]

5.2.2. The number of attacks is limited - deliberately or due to failure.

It cannot be excluded that Russia may have planned a three-day invasion of Ukraine, extensively using cyber-means in the prelude to 24 February invasion, but limiting these in the days thereafter, simply because kinetic weapons are more effective and efficient to

[101] Laurens Cerulus, "Kyiv 's Hackers Seize Their Wartime Moment," *Politico*, 2022.
[102] 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." p. 2.
[103] Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," *Carnegie Endowment for International Peace*, no. November (2022).
[104] Nadiya Kostyuk 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. pp 509-510.
[105] Joseph Marks and Aaron Schaffer, "11 Reasons We Haven't Seen Big Russian Cyberattacks yet," *The Washington Post*, 2022.

achieve taking Kiev and controlling Donbas.[106] This is in line with Russian doctrine[107] and besides 'you can't hold ground in cyber'.[108] Military and a limited number of cyberoperations might have been planned in tandem whereby cyberoperations primarily intended to shape the battlefield and create the conditions for a successful military intervention.

A second reason can be that cyberattacks may have been planned as a back-up scenario awaiting to be executed.[109] Digital undermining attacks may have taken place already, but their effects are yet to set in. 'Logic bombs' might have been placed lying dormant just until they are remotely activated or when particular conditions are met to automatically trigger their payload.

Thirdly, Russia might be able to use hard-cyberoperations against Ukraine but are reticent to do so because executing cyberoperations would give away their information position in their strife against other audiences especially NATO and EU member states. While there is no absolute need for stealthy operations during the war with Ukraine, cyberattacks against other states or entities require covertness in order not to give away modus operandi, nor scarce 'zero-day vulnerabilities and exploits'.[110] Moreover, the Ukrainian ICT infrastructure might be of use for Russia now or in the post-war phase.[111]

Fourth, cyberweapon's inherent characteristics of reach, time, speed and versatility are instrumental in the element of surprise,[112] especially when used in a supporting role in a wider effort to achieve an attacker's objectives. While cyberattacks can be conducive to subversion – as during the prelude to the invasion - Russia realised that cyberattacks have less strategic utility to contribute to the vital interests of the state compared to kinetic attacks, especially in a war-like scenario.[113] The efficacy of cyberweapons pales into insignificance when it comes to kinetic effects in during armed conflict. The absence of operational and tactical cyberweapons is, therefore, perhaps not even so unexpected.

---

[106] Robert Johnson, "The First Phase of the Russian Invasion of Ukraine 2022," *Oxford Changing Character of War Centre*, 2022.

[107] Johnson. What Mattson calls 'spear-point' warfare, related to the so-called sixth generation warfare. See: Peter A Mattsson, "Russian Military Thinking - A New Generation of Warfare," *Journal on Baltic Security* 1, no. 1 (2015): 61–70. pp. 62-63.

[108] Referencing to Tobias Ellwood, chairman of the committee of the House of Commons, see: Adam Bienkov, ""The Old Concepts of Fighting Big Tank Battles on European Land Mass Are over' Said Boris Johnson Last November, as He Mocked the Idea of Armed Conflict Returning to Europe," Twitter, 2021, https://twitter.com/AdamBienkov/status/1497139951552671744.

[109] Jason Healey, "Why No Major Onslaught? Here's a Thread on Various Reasons We've Heard," Twitter, 2022.

[110] 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.

[111] G. D. Vynck, R. L. C.. Zakrzewski, and C Zakrzewski, "How Ukraine's Internet Still Works despite Russian Bombs, Cyberattacks.," *The Washington Post*, March 29, 2022.; Cairan Martin, "Cyber Realism in a Time of War," *Lawfare*, no. March (2022).

[112] In contrast to kinetic weapons, the effects of hard-cyberweapons can be hardly visible with the human eye, or sometimes only be discovered months after their deployment.

[113] Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (2021): 51–90.; Gavin Wilde, "Assess Russia's Cyber Performance Without Repeating Its Past Mistakes," *War On The Rocks*, 2022.

Fifth, whilst Russia has a fair amount of cyber-related agencies within intelligence services of the state and armed forces,[114] or liaised to the state,[115] their capacity still has limits. First of all, Russian cyberoperations are large directed against three audiences; domestic, former Soviet republics; and NATO (and EU) and its member states.[116] Second, the agents working in the Russian cyber entities, as in many states, have a division in labour: not each hacker masters all techniques. Finally, aside from proxy entities, Russia allegedly made use of services of rogue or criminal entities such as the Conti group. The latter was made up of (amongst others) Russian and Ukrainian hackers, the linkage and therewith the effectiveness of this group perished after the Russian invasion when pro-Ukraine Conti members started leaking sensitive Conti data, exposing its code, methods and members.[117]

Another reason is that Russia want to avoid escalation. Russia is willing and able to unleash devastating cyberattacks. However, the risk of unintended and unexpected 2nd and 3rd order effects beyond Ukraine's cyber borders could be too great. The aforementioned 2017 'NotPetya' cyberattack initially targeted Ukraine but, by virtue of its design,[118] the malware rapidly spread worldwide. Striking the US or other NATO member states unintentionally with disruptive and indiscriminate cyberattacks may elicit unintended responses.[119]

A final reason might be that Russia has no 'cyberweapons' for wartime. Recent armed conflicts (e.g. Georgia, Syria, Ukraine) show that Russia prefers conventional kinetic weapons rather than using destructive hard-cyberoperations. Russian doctrine values the use of plausible deniable stealthy cyberattacks in peacetime, but once an all-out war commences, they are deemed to have lost its usefulness. When executed, hard-cyberoperations were conducted segregated from the kinetic fights.[120]

The limited number of cyber-attacks can be borne out of deliberate consideration but can also simply be due to miscalculation or failure. Hardly any plan survives first contact with the enemy and the Russo-Ukraine war appears to be no exception to that rule. Poor intelligence assessment by Russia, unexpected resistance by the Ukrainians and unforeseen support from non-state actors undermined the initial Russian plan. After the initial plan for a three-day invasion failed, Russia had to revisit and re-orchestrate their plans.

---

[114] 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), Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabiliites", Center for European Policy Analysis (CEPA), September 2, 2022, pp. 4-5.

[115] Including private entities, both legitimate and criminal. See: Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabiliites", Center for European Policy Analysis (CEPA), September 2, 2022, p. 4.

[116] Herbert S. Lin, "Russian Cyber Operations in the Invasion of Ukraine," *The Cyber Defense Review* 7, no. 4 (2022): 31–46. pp. 36-38.

[117] Jurgita Lapienytė, "Conti leaks: pro-Ukrainian member exposed more gang's chats and Trickbot's source code", Cybernews, 1 march 2022.

[118] An uncontrolled, self-propagating worm in combination with a global IT vulnerability.

[119] A cyberattack on any member of the Alliance could trigger Article 5.

[120] Nadiya Kostyuk and Yuri M. Zhukov, 'Can Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?, Forthcoming in *Journal of Conflict Resolution* (this version: September 22, 2017) pp 19

Designing and developing cyberweapons that create surgical effects is a time-consuming endeavour. Gathering actionable intelligence about an actual target, its computer and network infrastructure, hardware and software, determining the desired effects to be created, the methods and techniques to penetrate a system, or rather, successfully completing the entire 'cyber kill chain' requires months or even years of preparation time. Cyberweapons with strategic effects can be prepared in peacetime but after the failed invasion, the dedicated state-actors involved in cyber-activities may have lacked the required preparation time to produce effective hard-cyberweapons. Though some ill-prepared efforts were made targeting energy, finance or commodities (Ukrainian power grid attack), these operations had an ad-hoc characters and were not synchronised with other instrument of power.

The most challenging endeavour in an on-going (military) campaign is the coordinated and synchronised employment of elements of power in order to achieve a goal. When assessing the Russian invasion in Ukraine, the prelude to the war appeared to be a political-strategic plan executed at the level of president Putin, in which all instruments of power were planned to be executed in a more or less synchronised manner. After the decision to invade Ukraine, the command was transferred to the highest military commands.[121] This inevitably means a focus on the military instrument of power and a shift from a hybrid approach centred around a society-wide psychological warfare to a classical Russian military operation.[122] This would explain the lack of synchronisation with other instruments of power including hard-cyber operations which became manifest after the initial three days of the planned operation.

6. Conclusion

The main quest in this article was to assess what sorts of cyber-activities were executed in the run-up and execution of the Russo-Ukraine War, and why this war deviates from our expectation that the next war would be a cyberwar.

The conclusion is that cyberoperations were used both in the prelude to and during the war, but in a different manner from what was expected. While Russia was engaged in severe hard-cyberattacks in the period between 2014 and 2021 and in the run-up to the war on 24 February, it was expected that - given the reputation of the aggressor – more undermining or hard-cyberoperations would be executed. The dozen of destructive hard-cyberattacks that were launched just prior to the war and shortly thereafter, simultaneous with the ground offensive, originated in the cyber state actors' premises. The hard-cyberattacks with executed during the war, mainly originated from non-state actors and had less impact.

[121] Lawrence Freedman, "Why War Fails," *Foreign Affairs* 101, no. 4 (2022): 10–23.
[122] Seth G. Jones, Philip G. Wasielewski, and Joseph S. Bermudez, "Russia's Losing Hand in Ukraine," *CSIS Briefs*, 2022.; Mattsson, "Russian Military Thinking - A New Generation of Warfare." pp. 62-63.

Soft-cyberattacks have been engaged persistently in the prelude and during the war as could have been expected. The use of framed information and narratives via social media is however less coordinated than foreseen. The chaotic course of the war might have been inducive to a more reactive form of influence operations via cyberspace. The most prominent readjustment to the template of the Diamond model however is the unexpected engagement of non-state actors siding with one of the warring states. The engagement of these hacktivists and commercial parties, which actions cannot be attributed to a (warring or neutral) state, was not yet part of the rulebook of cyberoperations.

The use of instruments of power in cyberspace not only deviated from what was expected in *this* war, many researchers and experts also appeared to be – paradoxically enough - surprised about the kinetic nature of the war. Not least since it was expected that the next war would be a fully fletched cyberwar.

Two explanations for this view could be deduced. First, expecting the next war to be a cyberwar could very well be the result of a myopic self-fulfilling prophecy which oppresses sound military logic. Overestimating the Russian capacity in cyberspace, combined with internal turf war in Western administrations[123] how to prioritise capabilities for conflict, might have been inducive to our conviction that future wars will be fought (solely) in cyberspace. However, if one follows reason, invading another state will almost certainly entail kinetic elements of warfare. A second, adjacent, reason is that cyberoperations can have a severe impact, even a strategic impact as was witnessed in the (societal impact of the aftermath of the) 2016 US presidential election, or the nation-wide disruption of railway infrastructure,[124] but cyber-activities will not provide the decisive battle at the tactical level during a (conventional) war. Or as Lonergan c.s. recently put it: 'Cyber operations are a form of modern political warfare, rather than decisive battles. These operations don't win wars, but instead support espionage, deception, subversion and propaganda effort.'[125]

7. Discussion

What does this mean for the future of war? In a recent article Anthony Beevor argued that 'Putin doesn't realize how much warfare has changed',[126] as he is trapped in a World War II obsession. Though this is a fair point, it might similarly be valid for Western policymakers and academia. Several pundits of military thought saw the Russian invasion as a resurrection of the Cold War template, discarding the cumbersome new ways of warfare using buzz words such as influence, information, post-truth, hybrid, cyber, or cognitive. Subsequently, they assess the Russo-Ukraine War exclusively through the lens of armed conflict, conveniently neglecting the use of other instruments of power via other domains of

[123] Wilde, "Assess Russia's Cyber Performance Without Repeating Its Past Mistakes."
[124] Ryan Gallagher, "Belarus Hackers Allegedly Disrupted Trains to Thwart Russia Cybersecurity," *Bloomberg*, February 27, 2022.
[125] Erica D. Lonergan et al., "Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why.," *The Washington Post* March 7 (2022): 2022.
[126] Antony Beevor, "Putin Doesn't Realize How Much Warfare Has Changed," *The Atlantic*, 2022.

engagement. The fact that the next war did not turn out to be a cyberwar in the way it was expected, should not imply that one should relapse in preceding conceptual frames.

The authors argue that the Russo-Ukraine War underscores at least four elements, related to cyberoperations and the future of war.

First, a crucial lesson to be learnt is that competition, conflict or war is not fought in one domain (e.g. the land or sea domain) with one instrument of power (e.g. the military). **Contemporary conflicts are an engagement in all domains, all dimensions of the information environmen**t (physical, virtual and cognitive) **making use of all instruments of power available**. What can be witness in the future is an interplay and shifting prominence between the instruments, dimensions and domains. To affect an opponent, an aggressor will have to shift between kinetic and cyberoperations simultaneously altering from applying financial pressure to energy or creating uncertainty in compliance to international law. **The quintessential attribute in future wars is the ability to coordinate and synchronise all the element**,[127] in order to be effective. This is easier said than done as became clear after the first three days of the Russo-Ukraine War. For Western states and their forces, the current war should be an impetus to increase cooperation and sharing of intelligence between services, departments, military and civilian realm, and between states. Of note, for Western, rule-based democracies, the synchronised execution of instrument of power of a state is challenging since the different instruments, dimensions and domain are governed by diverse legal, ethical and political protocols. Autocratic regimes will experience less restrictions in executing these sorts of hybrid operations.

Second, though the use of hacker's groups, proxies and even commercial actors should not be overestimated,[128] they are an enduring reality in modern day conflict. **A proliferation of cyberactivity's and cyber actors can be witnessed**. These actors, ranging from malign cyber criminals[129] to *bona fide* hacktivists or multinational enterprises have interests that fluctuate amongst themselves and differ from the states they endorse. The result will be that states, hackers or commercial parties will only have volatile ad-hoc alliance, generating effects that appear to be aligned in a specific time and place. Once financial, physical or ideological interest fan out, so will the alliances. Moreover, it is no longer possible to attribute these non-state actors to a state. While the Sandworm APT or the St-Petersburg-based IRA (Glavset) can be linked to a state (Russia in this case), this does not apply to Anonymous, Conti or Microsoft. A development that will affect the applicability of the state-based systems of international relations and public international law. Stronger still, the activities of these actors will be inducive to the eroding of the use of force as a monopoly

[127] The instruments of power include diplomacy, military, economy or information; the domains are e.g. land, sea, air and cyberspace; and the dimensions are physical, virtual and cognitive.
[128] Chris Stokel-Walker, "Ukraine ' s Army of Hackers Failed to Thwart Russia and Quickly Gave up Group Subscriptions," *New Scientist*, 2022.
[129] Martin, "Cyber Realism in a Time of War."

of the state. While these actors will not engage in armed conflict itself, but they will engage in the wider conflict (or strategic competition) via cyberspace amplifying the previous argument. This, in turn, will expand the grey zone by increase the proliferation and democratisation of the use of coercion and violence.

Third, the development of cyberweapons that may create strategic effects requires ample preparation, intelligence gathering and development time. An effective manner of undermining military power is to affect weapon systems, command centres, radars or logistic systems. However, to pave the way for the development of operational or even tactical weapons, extensive knowledge about these systems is required which may require the involvement of these systems' manufacturers; with or without their knowledge. Therefore, to be effective in wartime, **a pro-active cyberspace posture in peacetime may be necessary**. Since new vulnerabilities and opportunities frequently rise, targets change, and offensive or defensive capability lose effectiveness over time, no advantage is permanent. To increase one's cyber resilience, 'persistent engagement'[130] – also in peacetime - may allow for greater freedom to manoeuvre in cyberspace. This may yet be a bridge too far.

Finally, and as a result, while during (armed) conflict the dominant lens of reference might be the **armed conflict** ('war'), this **does not and should not exclude other paradigms** that play a role in the wider conflict. After all, the fact that there is war ongoing does not preclude covert subversive actions in cyberspace, digital espionage or cybercrime in the context of a **wider strategic competition**. In fact, in future wars **all paradigms will overlap**. In the Russo-Ukraine War while only two states are at war, numerous actors are involved. Anonymous and the Conti group are not state-actors therefore public international law does not apply in full to them. This can, however, not mean that they have impunity by design; other legal regimes including national criminal law, privacy law or (international) human rights law will have to be applied in an assertive manner to address (potentially) undermining and illicit activities of these actors. Commercial ICT service providers will not only protect domestic ICT infrastructure in states adjacent to the war, but will also support warring factions, and intelligence agencies will take a forward leading stance taking sides in the war while avoiding becoming a belligerent party. For Western states this may imply that, though the differences between war and peace, internal and external security might exist in theory, in reality this distinction is obsolete which means that a revisit how the West prepares armed forces, or rather Western societies, against malign aggressors and attacks especially in the cyber-related information environment.

[130] Fischerkeller, Michael P., and Richard J. Harknett. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." The Cyber Defense Review, 2019, 267–87.

Our thinking about war and about cyberoperations in peace and war time is not set in stone. War studies are not an ideology, but they follow reason. If future conflicts thwart and falsify existing knowledge one must not start to dig-in but yield and evolve.