ÖMZ
seit 1808
ÖSTERREICHISCHE MILITÄRISCHE ZEITSCHRIFT
Online Only

JOSEF SCHRÖFL

The War in the Ukraine: Uproar in Cyber Space The Question of Information and Cyber Dominance

Abstract

The Russian invasion of Ukraine with its global consequences, from a humanitarian crisis resulting in millions of refugees, to the food crises in the Near East and in Africa, followed by a worldwide energy crisis generating economic shocks triggering geopolitical realignments which ultimately affect all military domains including cyber space!

Since the war started in Feb. 2022, Russia tried to bring down Ukraine to its knees in cyber space also. That article analyzes the issue of how Russian hybrid and non-hybrid cyber- and information warfare have played in Russia's favour, and where they might have failed but also, that the electromagnetic spectrum cannot be fully separated from cyber- and information space. This is an open analysis of an ongoing war, looking into the most important activities from both sides.

Table of contents

Summary

Cyber and information warfare is a fundamental element of the Russian military concept[1)], utilizing hybrid warfare capabilities. Over the past decade, Moscow has masterfully exploited the gray area between peace and war in its cyber and information operations. Some of these have disrupted the global economy, such as the 2017 ransomware NotPetya, which crippled many businesses in the West. Others were more espionage-oriented, such as the Solar Winds supply chain attack, a sophisticated targeted cyber operation against a company relevant for US national security and critical infrastructure. However, none of these attacks reached the level that could be described as crossing the threshold of armed conflict. These cyberattacks were accompanied by disinformation campaigns in which narratives such as "The impending collapse of the western world", "Threatened values - Russia, the guardian of decency and morality" or "Lost sovereignty over brother nations" were repeatedly used[2)]. The latter narrative was addressed by the Russian President, who described Ukraine as "Little Russian", part of an "all-Russian nation", or junior partner in a "triune Russian nation". Furthermore, he reportedly questioned Ukraine's identity and legitimacy for years and claimed conspiratorial views of Ukraine's identity[3)] as an "anti-Russia project" of the West in his 2021 essay "On the Historical Unity of Russians and Ukrainians"[4)].

Since the invasion, Russia has also tried to weaken Ukraine with cyberattacks on its critical infrastructure like on computer systems of the Ukrainian Ministry of Defense, banks and public administration. These attacks were accompanied by disinformation and misinformation campaigns, propagating the respective Russian narratives. In parallel, Ukrainian satellite communications have also been hacked at the same time, but, due to timely countermeasures, services could quickly be restored.

Events since the start of hostilities have made it clear that Cyber space, information space as well as the use of the electromagnetic spectrum need to be seen as an entity.

[1)] https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf (Unless otherwise indicated, all links were last accessed on 10.01.2023)

[2)] according to the task force of the European External Action Service "EUvsDisInfo", https://euvsdisinfo.eu/report/russia-fights-the-collective-west-not-just-ukraine

[3)] "Putin said, that Russians and Ukrainians "practically one people". Reuters. 29 August 2014. https://www.reuters.com/article/us-ukraine-crisis-putin-people-idUSKBN0GT14720140829

[4)] In Russian: „Об историческом единстве русских и украинцев", http://en.kremlin.ru/events/president/news/66181

Introduction

The Russian invasion of Ukraine has been and still is being accompanied by a cyber and information offensive. This working paper analyzes which party of the war is predominant in which matters and claims that all the attacks in Cyber space and information space are accompanied by attacks at and from the electromagnetic spectrum. Firstly, after giving background information on the subject, the paper examines the interdependence of cyber- and information war, using the electromagnetic spectrum. Thereafter, the paper will analyze these three related areas separately based on the attacks that have occurred so far during the war and will explain the connections. Finally, the question is pursued why Russia's previous attacks within these three domains fell short of expectations and closes with exploring solutions and recommendations for EU and NATO countries.

Background Information

On the morning of February 24, 2022, Russia's attack on Ukraine suddenly caught the West by surprise and confronted it with a reality it either had not realized or even neglected until then. Since then, especially the major Western states have been forced to abandon their state of self-deception that they had cultivated. In the meantime, other perspectives have become familiar to them. They are learning to see Vladimir Putin differently and they must understand that he did not just lie. The Russian president has always denied incidents of the past, among them plain murders, poison plots, and the many attacks on our western value system, for which he has used his private misnomed “truth” as a perfidious disruptive strategy.

That “truth” was coherently messaged in and of itself: Russia is always innocent of everything the West attributes to that country. Putin's mission is to save Russia and the Russian people from destruction because the West wants to destroy Russia. The invasion of Ukraine cannot be understood without Putin's view of history. In his view, Russia has been challenged to assert itself against enemies from the West for 1000 years and thereby gained its strength - most recently during the Second World War. Putin accuses the West of denying Russia's world power status beginning in 1990[5)]. This world view results in a permanent diffuse sense of threat. To pursue his goals, Putin has merely reactivated old KGB methods from the Soviet times, including:

- Disinformation and misinformation, i.e. the continuous dissemination of fake news on all possible channels. In recent years, the Kremlin has also built up its own media industry with broadcasts

[5)] See also: Angela Stent: “Putin's World : Russia Against the West and with the Rest”, 2020, Twelve, US, p12-25

over RT and Sputnik in order to influence opinion abroad. A specific feature of Soviet as well as current Russian disinformation is the reinterpretation of events.

- Sabotage: The goal is to confuse the enemy by destabilizing the enemy's population's trust in the government's ability to guarantee the basic needs of life. State actors, moreover, work closely with organized crime which is a general feature of Russian hybrid warfare[6)].

In contrast to the Soviet era, however, nowadays new and additional "digital fire accelerants" are available to Moscow in the form of the Internet and social networks.

In practical terms this means that the Russians are conducting an ever more intense cyber and information war, including the electromagnetic spectrum: The systematic distribution of psychologically and ideologically screened material of provocative character and a mixture of partly true and false information accompanied by attacks on the critical infrastructure can create mass psychosis, lead to despair and generate a mood of doom, thereby undermining confidence of the target populace in their government and armed forces. These measures clearly serve a nihilistic ideology of pure power.

The Interdependence of Cyber- and Information war, using the electromagnetic spectrum

Cyberwar is on the one hand the military conflict in and around the virtual space, the Cyber space, and includes all measures of information and communication security technology as well as all measures to ward off sovereignty-endangering cyberattacks. Endangering sovereignty may come as cyberattacks on military ICT systems as well as on critical infrastructures and / or constitutional institutions. On the other hand, cyberwar refers to the high-tech forms of war in the information age, which are based on extensive computerization, electronic systems and networking of almost all civil and military areas and domains. Consequently, the battle for (the right) information - including information warfare - takes mainly place in Cyber space. The manifestations of information war are known as deep fakes, disinformation and misinformation campaigns and operations as well as psychological operations (PsyOps). All these elements can be interrupted or disturbed via the electromagnetic spectrum, for instance by attacking satellite communications.

Cyber space does, however, offer defensive options, too: Fake information can also be countered by means of the Internet. As excellently demonstrated by Gen Nakasone's US CyberCommand during the

[6)] Like described from James O. Finckenauer and Yuri A.Voronin in "The Threat of Russian Organized Crime", NCJ 187085 from June 2001

US elections in 2016, when dozens of social media accounts on Twitter, Instagram, etc. were simply shut down using military computer network attacks[7)].

The same can also be seen in the current war in Ukraine: common cyber-attacks such as ransomware, DDoS attacks, use of crypto apps, malware, compromise of information systems, 0-day cross-platform worms, SCADA attacks, etc. were used by both sides, to influence the adversary, cause damage or cause cumulative costs (see below). Simultaneously, disinformation and misinformation campaigns are being pursued.

To understand Russian citizens' world view, it is mandatory to speak Russian and to watch Russian TV. Kremlin control permeates every part of Russian TV. During daytime all mundane programs have been substituted by tenacious propaganda about Russia's place in the world, the threat posed by the liberal but weak West and the "liberation" of the Ukraine from Nazis. "The Bandera elites must be liquidated; they cannot be re-educated. The societal swamp that supported them must experience the terror of war, learn the lesson, and pay for its guilt"[8)] was and is still one of the main messages from Russia and serves the narrative of Russia's "threatened values". This narrative is also used to criticize progressive Western values such as the rights of women, ethnic and religious minorities or the LGBTQ community. According to pro-Kremlin disinformation outlets, the western world is destroying fundamental values through decadence, feminism and political over-correctness. Russia, on the other hand, is the guardian of decency and morals[9)].

The electromagnetic spectrum has been used for interfering and/or disrupting the adversary's flow of information. Russia tried to cut the Cyber space within the Ukraine by shutting down their server and mobile connections like 3G/4G-band, to disturb their national command and control systems thereby inhibiting Ukraine's timely response to Russian fake information.

One of the main intents of Russian propaganda activities is to "dehumanise" the other side. Targeted means of influencing serve as part of psychological warfare, a common method in times of war. From now on, these narratives[10)] determine how and what the West should think about a crisis/war and what judgment/evaluation to make. Many observers agree that Ukraine's conflict with Russia - an

[7)] https://www.c4isrnet.com/cyber/2021/03/25/us-military-conducted-2-dozen-cyber-operations-to-head-off-2020-election-meddling/

[8)] https://www.watson.ch/international/russland/444993013-nachrichtenagentur-des-kremls-ruft-zur-vernichtung-der-ukraine-auf

[9)] according to the task force of the European External Action Service "EUvsDisInfo", https://euvsdisinfo.eu/report/russia-fights-the-collective-west-not-just-ukraine

[10)] The author understands "Narratives" as overall messages that are spread and constantly repeated in the form of individual texts, images and videos by fake accounts in social networks or on supposed news portals. Individual reports always contribute to a message, a narrative. Some of these narratives have been used for many years, combined or altered according to current events and settings.

established cyber superpower that isn't hesitant about flexing its muscles aggressively - could test the rules of war in new and unexpected ways, while some say it already has done so[11)].

Cyber is the new battlefield and its means that information operations should no longer be seen as soft power projection but should be considered as hard powers just as military means, although NATO and EU still do not have a clear perception on this topic. The question remains whether it is one new comprehensive domain or maybe it is better to regard them separately[12)]. The same applies to the electromagnetic spectrum.

The electromagnetic spectrum, information and Cyber space reside within the physical dimensions of the information environment and can be used as sites of warfare, equivalent and akin to the domains of land, air, sea, and space.

In the present author's perspective, these domains are of equal value, whereby it must always be considered that one can influence the other and that information or electromagnetic attacks cannot be that successful without using Cyber space[13)]. The relationship between the respective elements can also be summarized with a comparison: It is a threaded pipe in which water flows. The thread is the electromagnetic spectrum, the pipe is the Cyber space, and the water represents the information flowing in it[14)].

Therefore, the electromagnetic spectrum cannot be fully separated from Cyber space and information space.

[11)] https://www.cyberscoop.com/russia-ukraine-cyberwar-nato-geneva-microsoft/

[12)] Germany f.e. sees it together (https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum). GB and the the US not (https://www.cybercom.mil/, https://www.ncsc.gov.uk/)

[13)] Therefore I mostly agree with Stefan Libicki´s essay from 1995: "Is there an elephant? Seven forms in search of a function: Command-and-control warfare, Intelligence-based warfare, Electronic warfare, Psychological warfare, Hacker warfare, Information warfare, Cyberwarfare" (https://apps.dtic.mil/sti/pdfs/ADA367662.pdf)

[14)] See also Nicolas Mazzucchi "AI-based technologies in hybrid conflict: The future of influence operations", Hybrid CoE Paper 14, June 2022.

The electromagnetic spectrum

Listening to stories from Russian soldiers, one can get the impression of an army that is having major problems in communicating and coordinating, as the following examples illustrate:

"This is Kaspi-23," says a soldier. "I don't understand you. I can't hear you, I repeat, - I can't hear you." Once someone complained about the lack of artillery support. "I told you to send the damn grenades. Confirm!" he says - "Whom did you tell that?" came back. Not only that the Russians misunderstood each other, they were also disturbed in the process. When Ukrainians spotted the frequencies, they bombarded the Russian soldiers with propaganda or blared the Ukrainian national hymn through the channel. In one case there were only grunting pigs to hear. The soldiers try in vain to yell at it. Sometimes Ukrainians directly insult Russians. "Go home!" is one of the kindest things they are confronted with[15].

But there is also an invisible battle for radio dominance ongoing. Both sides are trying to block the adversary's radio and radar systems. Still, with advantages for the Ukrainian side, since they, among other things, have used cyberattacks to disable Russian drones, which pose as Russian fighter jets by using false identifiers, and in some cases, they have even been able to take control over drones[16].

But why and how is the electromagnetic spectrum and the Internet in the Ukraine still existing, - why hasn't it not been destroyed by Russia?

First, - Starlink, a company of the US-American business magnate Elon Musk, which offers Internet access via its satellite network, comes into place. Several thousand Starlink terminals are currently in use within the Ukraine to support and maintain the local mobile network. Even Elon Musk recently publicly rolled out the idea of turning off the system again because it would cost him, the richest man in the world, an enormous amount. He also posted a peace plan for Ukraine on Twitter, which must have caused extremely satisfied faces in Moscow. In it he suggested that Crimea should remain with Russia ("that was Khrushchev's fault," he argued) and that the people of Donbass should vote whether they would rather belong to Russia or Ukraine. Some days later he denied. His satellite network is still working at his cost.[17]

Second, - because on the day of the invasion (24th of February) - three long planned key decisions took place:

[15] https://www.abc.net.au/news/2022-06-09/mobile-phones-are-changing-the-way-war-is-fought-in-ukraine/101085610

[16] https://www.nzz.ch/international/der-elektronische-krieg-in-der-ukraine-unsichtbar-aber-wichtig-ld.1688611?

[17] https://kurier.at/politik/ausland/elon-musk-ukraine-russland-putin/402186138

1. The Ukrainian Telecom regulator (NKRZI) had allocated the Ukrainian operators additional 3G and 4G frequency bands. This increase of frequencies meant that the whole country benefited from that extra capacity, especially during the first wave of refugees.

2. The Ukrainian mobile operators and the Telecom companies decided not to suspend any account if it would run out of credit. That meant, that all soldiers (but also refugees and the entire population) has always been able to communicate.

3. All Ukrainian mobile operators and the NKRZI, suspended all inbound roamers from Russia and Belarus. That meant, that Russian and Belarussian mobile networks could not be used for roaming anymore.

Taken together, these are key reasons, why Russia has not yet been able to disrupt Ukraine's cellphone network and internet, neither with hacking nor bombing. Russian soldiers need it for their communication as well! Smartphones can be found with all soldiers involved in the war. But Cell phones are pinging signals to the nearest radio tower, allowing both Ukraine and Russia to track the movements of enemy forces. In this case, the Ukrainian side has an advantage because it owns the domain in which this radio traffic takes place and has the means to evaluate them[18)].

Most recently, NATO has supplied Ukraine's armed forces with anti-drone jammers. The jammers are part of a comprehensive support package, Secretary General Jens Stoltenberg told the public on November 25th at a press conference in Brussels. In particular, the jammers are intended to help Ukraine fend off attacks with kamikaze drones. The devices are usually electromagnetic transmitters that interfere with the drones' navigation or communication systems, but could also be used for interfering with the Russian tank and/or artillery command and control systems[19)].

The Information space

Vladimir Putin's information space army of trolls, cybercriminals and warriors has shown the Western world their destructive power for years. Their cyberattacks have interfered in countless elections and referendums, with Brexit and the 2016 US elections being the outstanding examples[20)]. They hacked western computer systems, spread viruses like NotPetya (one of the most disruptive cyberattacks in history) in Ukraine in 2017 and attacked western critical infrastructures like SolarWinds 2020 or

[18)] https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

[19)] https://orf.at/stories/3295244/ The Russian army has been increasingly attacking Ukrainian critical infrastructure with kamikaze drones since October 2022, using mainly Iranian-made aircraft Shahed-136. It has a triangular wing and is equipped with a warhead. The drone is usually launched from trucks and crashes towards its target at high speed, but can be interfered by electromagnetic attacks.

[20)] https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

Colonial pipeline 2021[21]. But they also sponsored conspiracy theorists and right-wing hardliners if you look at the stories about Q-Anon or western coronavirus vaccines.[22]

However, when the time came to oversee Putin's most ambitious and probably most important operation, the information space army appeared to have failed on all fronts. The goal has been to spread false information and to attempt to manipulate society, to push for actions that can destabilize the country during the war. But rather than the narrative of Russia as the Eastern leader fighting Nazis in Ukraine and protecting all ethnic Russians in the minds of Europe, Ukraine dominates so far, this online battle for the hearts of Westerners. And now it is very hard for Russia to change the narrative.

Nevertheless, the impression that Ukraine is clearly winning the "information war" or that it would dominate the digital discourse through informational self-defense is only true for Western observers. In social media in some African states, India, Pakistan or China, Russian disinformation actors are sometimes more successful in placing their narratives and memetic communication artifacts[23]. Russian propaganda can fall on fertile ground there because it also draws from negative cultural experiences in these countries. The fact that such an approach can then turn into the opposite was shown in September 2022 at the summit of the Shanghai Cooperation Organization (SCO) in Samarkand, where many of the region's countries now look at China, not Russia, as the helping hand in development assistance.[24]

However, after many years of a far disproportionate dominance of Russian and European right-wing extremist propaganda - the two can often hardly be distinguished - the tide has turned mostly, especially on social media like Facebook, Twitter and Instagram. Since the outbreak of the war, attempts have been made there, to circulate conspiracy narratives justifying the Russian invasion. The most common of these were that Putin had to invade to dig up secret bio-labs in Ukraine, where even more secret chemical and biological warfare agents were being produced on behalf of the CIA[25]. All of this seems somewhat spasmodic, and the spread of such fake news is more than limited and not successful. The sheer visual power of war videos makes it difficult to establish narratives that compete with these videos in the infosphere.

The Russian Duma, meanwhile, passed a law providing prison of up to 15 years for publishing “false information” about Russian state operations. The law, passed by the Moscow Duma in its third reading,

[21] https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

[22] https://www.politico.com/news/magazine/2022/03/12/ukraine-russia-information-warfare-likewar-00016562

[23] https://carnegieendowment.org/sada/87353

[24] https://www.politico.eu/article/russia-disinformation-africa-europe-sergey-lavrov/

[25] https://www.bbc.com/news/60711705

sets prison terms and fines for people who "knowingly spread false information" about actions by Russian government agencies "outside Russian territory"[26].

However, after a break around the primary attack on February 24th, Russian disinformation and misinformation campaigns and attacks have come back at a high level. The floated fake news on the European population from September 2022 to denigrate the neighbors to the police if they heat their apartment over 19 degrees was unsuccessful, because nobody believed these “news” and governmental authorities reacted immediately on social media[27]. Also, the recently launched disinformation campaign with Minister of Defence Shoigu as front man, who after a six-month break called his counterparts in the US, UK and France accusing Kyiv of wanting to detonate a radioactive, "dirty" bomb without presenting any kind of evidence, also failed because the US, France and the UK called the claim about a "dirty bomb" clearly false. A joint statement by the foreign ministers of these countries said “As a reminder, Ukraine does not have nuclear weapons! The world would see through any attempt to use this claim as a pretext for escalation.[28]”

The Cyber space

The war in the Cyber space had begun long before the first Russian troops crossed the border into Ukraine. Since 2014 Ukraine has registered more than 5,000 cyberattacks on state institutions and critical infrastructure[29].

By mid-2021, the hackers started to target digital service providers, logistics providers and supply chains in Ukraine and abroad to gain further access not only to Ukrainian systems but also to those of NATO member states. When in early 2022 all diplomatic efforts to de-escalate the conflict failed and the Russian military began to complete its troop deployment along the border with Ukraine, cyberattacks rapidly intensified. The hackers were also increasingly using wiper malware, which erases hard drives and data, against Ukrainian institutions[30].

Shortly after the invasion, websites of banks and government departments were attacked again in a next wave of attacks. At the same time, thousands of broadband users in Europe lost their Internet connection in a targeted attack on modems operated by the American satellite operator Viasat. The

[26] https://www.independent.co.uk/news/world/europe/ukraine-war-latest-russia-law-b2028440.html

[27] Neue Zürcher Zeitung (intern. Edt.), Donnerstag 15.September 2022, p6

[28] https://orf.at/stories/3291109/

[29] https://www.databreaches.net/security-service-of-ukraine-identified-fsb-hackers-who-carried-out-more-than-5000-cyberattacks-on-state-bodies-of-ukraine/

[30] https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

common goal of all these attacks was to shut down the command and control systems of the Ukrainian officials and especially of the military[31)].

Principally, the Ukraine has expanded and improved its capabilities in the last years. With support from some western nations, like Israel, Lithuania, the Netherlands, Poland, Estonia, Romania and Croatia, which sent cyber security experts to help Ukraine dealing with cyber threats[32)].

But Ukraine did not get only support from nations:

- The Anonymous collective immediately to support after the physical invasion. Starting with YourAnonNews, one mighty Anon account after another, which had been known for years, popped up on Twitter almost every day[33)]. As a starting present, the website of the Russian Ministry of Defense was hacked and data records that were hidden on the server were published, while the notorious "Killnet gang" pledged support for Moscow and threatened retaliation. Anonymous posted on Twitter on May 21 that "the collective is officially in cyberwar against Killnet". Shortly after Anonymous declared cyberwar, another message was posted saying that Killnet's website had been shot down. So far, around 45 hacker groups have become active for the Ukraine. Most of them are loosely associated with Anonymous. All groups are running ransomware, psyops, hack and leak, DDoS and defacement campaigns against Moscow[34)].

- Ukraine's Minister of Digital Transformation, Mykhailo Federov founded in late Feb. 2022 the Ukrainian volunteer-"IT-Army" operating on Telegram. Currently around 300.000 volunteer hacker from all over the world are supporting the Ukraine by attacking Russian media, broadcasting, companies, etc.[35)]

It clearly was Russia's desire to bring down Ukraine to its knees in Cyber space. Russian attacks did some damage, but nothing dramatic so far. DDoS attacks, in which European- and US- websites are deliberately overloaded with data traffic and thus become unusable, cyber-vandalism, in which websites are hijacked and redesigned can be observed as well[36)]. Some of them were also coordinated with kinetic attacks, such as attacks on cell phone providers in regions that were simultaneously being

[31)] SonntagsZeitung, Samstag 9 April 2022, S. 17

[32)] https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339

[33)] The largest accounts have over 15 million followers:
(https://www.derstandard.at/story/2000134361378/anonymous-sind-zurueck-wie-der-cyberkrieg-gegen-russland-ablaeuft)

[34)] https://orf.at/stories/3256364/

[35)] https://t.me/itarmyofukraine2022

[36)] https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

shelled by Russian artillery or more previously by attacks against the critical infrastructure[37]. But nothing has hurt Ukraine so much right now that it couldn't stay online. Russian hackers also managed successful attacks outside of the Ukraine. Noteworthy here are those attacks on government servers in Lithuania (May), Italy (June), Montenegro (August), Germany (September), Bulgaria and Poland (both in October)[38]. But none of them caused damage beyond repair.

The fact that the Russian elite hackers with catchy names like “Fancy Bear”, “Snake”, “Sandworm” or “Killnet” have so far been able to cause relatively little damage only has even more reasons than Ukraine being well prepared for these attacks. Many experts observed the Russian attacks and made a devastating verdict. "Except for the satellite hack at the beginning of the war, all attacks were purely opportunistic. Nothing was thought out or well planned.” It seems, that the Russian online war is executed and fought similar to that on the ground: With brute force instead with finesse[39].

Why is the Russian “Cyber- and/or Information Pearl Harbor” still missing?

One of the biggest surprises of the war so far is the absence of a visible, full-scale cyberwar, - also in information space. Why has the IT superpower Russia not yet mobilized all its cyber- and information warfare potential in the war against the Ukraine? Why did “Cyber Armageddon”[40], or “Cyber Pearl Harbor”[41] not happen so far? From the authors perspective, there are three explanations possible[42]:

Time Hypothesis: To cause greater damage, attackers would have to wait in the well-protected networks of western companies and authorities to detonate their “virtual bombs”. However, even powerful and well-trained cyber armies of western states would need at least a year for preparing such programs and would also be prone to espionage during that time. Russia's hackers may have had much less time. Thus, the cyber and information warriors no longer found the necessary attention and

[37] https://www.ohchr.org/en/press-briefing-notes/2022/10/ukraine-attack-civilians-and-infrastructure

[38] https://orf.at/stories/3284892/ as well as https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland

[39] See the interview with Marina Krotofil: https://securityboulevard.com/2022/08/bsidestlv-2022-marina-krotofils-kinetic-and-cyberwarfare-twins-siblings-or-distant-relatives-or-why-bombs-speak-louder-than-electronic-bits/

[40] Or cyber apocalypse: Implies that critical infrastructure within one or more countries is continuously bombarded with ransomware and other attacks so that every civilian service is either dramatically slowed or shut down.

[41] The term was coined in 2012 by U.S. Defense Secretary Leon E. Panetta and aims to relate the intensity and potential devastation of a major cyber-attack with the 1941 attack on Pearl Harbor, a surprise military attack by the Japanese Navy against the U.S.

[42] Thanks to Stephanie Carvin for sharing her article: “How to Explain the Failure of Russia’s Information Operations in Ukraine?” from March 2022 (https://www.cigionline.org/articles/how-to-explain-the-failure-of-russias-information-operations-in-ukraine/). Her thoughts inspired me for that conclusion.

support from the Kremlin, because the military build-up in the other domains (land, sea and air) needed all of Russia's power.

Preparedness Hypothesis: Kyiv may have learned the lessons of 2014 and is better prepared, due to the help from western states and non-state actors. For instance, Microsoft is helping Ukraine by taking over Internet domains from the Russian hacker group Strontium (affiliated to Killnet) and redirected attacks into so-called "sinkholes"[43]. That would presuppose that the Western world was also better prepared for the Russian cyber and information war machine.

Uncertainty Hypothesis: That solution would turn out to be the most unpleasant and dangerous. Cyber Armageddon is simply invisible, - the Russian cyber and information warriors would have had enough time and support from Moscow to prepare a large-scale attack and implemented the Virus already in our networks. But we do not know about it and Putin is just waiting to trigger it.

But no matter which hypothesis would eventually turn out to be the correct one, the lessons from Ukraine call for a coordinated and comprehensive strategy from EU and NATO to strengthen defenses against the full range of cyberwar destructive, espionage, and influence operations.

Conclusions and recommendations

Since the annexation of Crimea in 2014, it was believed that Russia had created a new form of modern warfare. Without firing a single shot, Putin's troops took control of the Ukrainian peninsula, which was considered the new gold standard for warfare through hybrid warfare especially with cyber means - a war in which tanks are not the focus, but instead disinformation, cyberattacks, sabotage and special forces. No one in NATO and/or EU had believed Moscow would be capable of such an operation, everyone had been taken by surprise. But it is now apparent that the Russians are not as far along as assumed. The underestimation of the Ukrainian public will to resist led to the fact that the hybrid attack on Ukraine become a hybrid war which went rogue, and which is now also a conventional war.

However, also in this war, the cyber and information space, using the electromagnetic spectrum is still one of the most important parts of the battlefield, it's not just only about pure propaganda.

What should the NATO, the EU expect in the future and what could be done?

The Western world is likely to be prepared for a protracted, mostly low-intensity war. Putin already perceives the imposition of sanctions almost as a declaration of war. For Russia, the tool of retaliation

[43] https://www.csoonline.com/de/a/microsoft-uebernimmt-domains-von-russischen-hackern,3673868

could be cyber and disinformation operations. In its latest report from Dec. 3rd Microsoft warned of an increase of Russian military offensive cyber operations (wiper malware) against European critical infrastructures[44] in the next months. Collective Western efforts towards cyber resilience, both at national, EU and NATO level, therefore, urgently need to be stepped up.

The cyber threat landscape is evolving at a rapid pace. Europe and the US must now prepare for ongoing gray area conflicts. Only through anticipation, risk mitigation, and creativity can they shift the balance of power in Cyber space in favor of the defenders of a whole, safe, and free Internet.

EU and NATO countries should develop satellite capabilities to provide coverage and connectivity to the global internet. This would become part of a global doctrine to encourage open information provided in conflict zones and authoritarian internet shutdowns. The logic should follow that of Cold War shortwave radio[45].

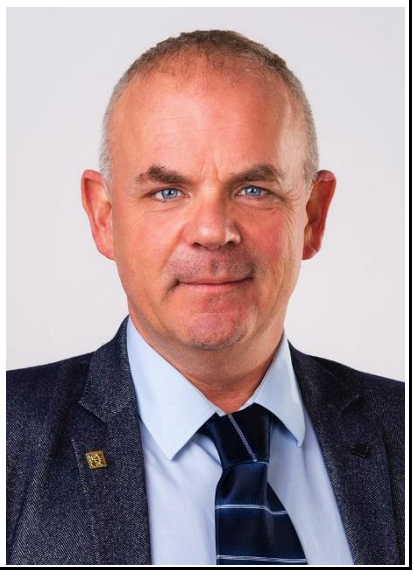
Whoever wins inside the Cyber space decides what people and societies believe and what they think truth looks like but also, what is happening physically on the ground. Because whoever loses the battle for information also loses the moment to act and win the physical war. Currently it seems that Russia's prospects to win this war are not too bright, not even in information and Cyber space.

[44] https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

[45] https://coldwarconversations.com/episode239/

The Author

HR Dr. Josef Schröfl, ObstdhmfD dM



Born 1962; HAK und HTL Matura, EF 1982, sine then long-standing militia career with the LWSR21/JgRWien, most recently BaonKdt JgB4; MA "International Politics", University of Delaware/US , Dr. in political science/public economy at the University of Vienna; several assignments with AUSBATT/UNDOF, most recently SSOPers 1995 - 1996; 1996-2006 employed as adjutant at the National Defence Academy/Vienna; 2006-2018 Military Strategy Division in the AUT MoD heading ULV/USV, Cyber Defense and New Threats; since 2019 Deputy Director CoI Strategy & Defense at the Hybrid Center of Excellence in Helsinki/FIN. Author and co-author of several books and published numerous articles on the topic of asymmetric warfare, Cyber and new threats.