Volume 3, No. 1

2024

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE

GUEST EDITOR: Prof. Jacek Leśkow Ph.D

Special Issue on The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure

NASK

ISSN 2956-3119
E-ISSN: 2956-4395

Volume 3, No. 1

2024

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

NASK

www.acigjournal.com

Special Issue on *The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure*

Guest Editor: **Jacek Leśkow**
Managing Editor: **Marek Górka**

Printing:

ISSN: 2956-3119
E-ISSN 2956-4395

Information email: contact@acigjournal.pl

Table of Contents

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Introduction to Special Issue on

The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure

Jacek Leśkow | American University Kyiv Ukraine |
ORCID: 0000-0003-2228-393X

Received: 12.02.2024

Accepted: 24.05.2024

Published: 23.07.2024

Cite this article as:
J. Leśkow "Introduction to Special Issue on The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure" ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/191475

Corresponding author:
Jacek Leśkow, Rector, American University Kyiv Ukraine. E-Mail: xyz@abc.com;
0000-0003-2228-393X

Dear Readers,

I am pleased to introduce a special edition of *Applied Cybersecurity & Internet Governance* (ACIG) journal dedicated to the Russian-Ukrainian war and the associated cybersecurity risks. The conflict started by Russia in 2014 with illegal annexation of Crimea and a part of Donbas region has a profound implication. Our civilisation shifts to the digital dimension; therefore, understanding cybersecurity within this context has become more critical than ever.

I would like to invite readers to reflect on some key questions: How did the Russian-Ukrainian war emerge after a prolonged period of peace? What political processes lead to the loss of tens of thousands of Ukrainian lives, the displacement of hundreds of thousands in Ukraine, and the migration of millions of Ukrainians seeking refuge in the European Union (EU) and North America? The answer is, however, that it is essential to identify crucial factors contributing to the current crisis, also in cyberspace. The first fundamental factor is the lack of strong moral condemnation of the Soviet system based on communist ideology. Unlike luminaries of fascist regimes, communist perpetrators were never held accountable for their horrible crimes committed in the 20th century. Historical research proves that Stalin and his followers were responsible for the deaths of at least three times more innocent civilians than Nazis. While Nazi German concentration camps are presented as historical sites, Soviet *gulags* are not memorised similarly. Some Western intellectuals have even supported Soviet-style communism. For instance, a major plaza in Naples, Italy, was named after Togliatti, an Italian-born communist and a strong supporter of Stalin.

After the collapse of the Soviet system, many Western countries did not insist on moral accountability for crimes committed by communists. Instead, Western elites moved to the 'business as usual' approach that resulted in two fundamental flaws of Western policy with respect to Russia. These two biggest flaws being the reset policy with Russia originated by US elites and the Nord Stream gas pipeline, a Russian-German cooperation. Both reset policy and Nord Stream initiatives were strongly supported by decision circles of the West after Putin attacked Chechnya, brutally killing tens of thousands of innocent civilians. No change in reset or Nord Stream was done after Putin's Russia attacked Georgia, annexing 10% of its territory. Therefore, in the criminal mentality of Putin and his aides, such an approach of the West was understood as condoning every crime of Russia as long as cheap gas flows in and hundreds of millions of euros per day flow to Russian accounts.

This policy enabled Russia to rebuild its military strength with financial gains from gas exports to Western Europe, facilitating a resurgence of Russian imperialism with the consistent support of Western political elites.

Another fundamental factor in the Russian-Ukrainian war is the Ukraine's aspiration for independence and alignment with the EU. Since the early 2000s, I have frequently visited major Ukrainian universities, such as Kyiv, Dnipro, Odesa, and Lviv. The first significant shift from the communist past occurred during the Orange Revolution in 2004. Although Ukraine then was still divided, with the West being pro-European and the East more pro-Russian, democratisation had begun, and the Stalinist past has been criticised widely. Symbols of communism, such as the statues of Lenin, were finally removed, and new West-oriented political and economic elites have emerged. In my frequent meetings with Ukrainian academics and business people I was asked the question regarding the successes of democratisation in Poland. I realised then that my home country, Poland, was an example to follow for Ukraine. The second, even more significant breakthrough in recent Ukrainian history was the Revolution of Dignity in 2014. Ukraine then has turned out to be more unified in the desire of being pro-European.

So, in recent decade we have seen two conflicting trends. The growth of the totalitarian regime in Russia was financially supported by Western political elites and the strong pro-independence, anti-totalitarian attitudes of Ukrainian elites. The sheer existence of democratic Ukraine, where many among political elites were first-language Russians (President Volodymyr Zelensky being the most prominent example), was an existential threat to imperialist Russia run by criminals such as Vladimir Putin and his closest aides. That is why Ukraine is such an existential danger to Putin's regime, and that is why Putin is using the potential of the Russian army to destroy Ukraine.

Understanding these historical and political circumstances is essential for comprehending the cybersecurity risks associated with the ongoing conflict. This edition of the ACIG aims to explore these risks in depth, providing valuable insights into the complex interplay between geopolitics and cybersecurity.

Putin's Russia, being the biggest terrorist organisation on our planet, represents a significant threat to global security, employing various means to disrupt the vital processes of numerous democratic countries. This capability is used deliberately and systematically to destabilise the digital value chains of our modern civilisation. Numerous cyberattacks on transportation or communication infrastructure have been attributed to Russian state- and non-state-sponsored actors. In response to these challenges, we remain united and resilient, with a firm belief in our ability to overcome hostile actions.

One crucial strategy to ensure our success is to conduct continuous research on the cyber threats posed by anti-democratic states. This objective motivated the preparation of this special volume of research articles dedicated to the Russian-Ukrainian war and its impact on cybersecurity.

In this volume, there are a total of 12 articles. The special issue opens with the article 'Russia's cyber campaigns and the Ukraine War: From the "gray zone" to the "red zone"'. The author clearly identifies the importance of the fifth battlefield – cyberspace combined with the traditional four dimensions: land, air, sea, and space. The author emphasises the danger of a hybrid war fought with all available means by the Russians. The importance of information warfare as an element of hybrid war is also emphasised in the second article, 'Moscow and the world: From Soviet active measures to Russian information warfare'. The author shows the key importance of information warfare used by Putin's Russia in waging the kinetic war with Ukraine and the cyberwar with democratic countries. It is, nevertheless, clear that the start of a full-scale war between Russia and Ukraine had an immense impact on global politics. How the so-called pariah states cooperate with China is a topic of our third article entitled, 'Collaborating pariahs: Does the Ukraine War cement and adversarial cyber-information bloc?' In our volume, the global aspects of the Russian-Ukrainian war are also accompanied with more specific discussions on information war and the so-called 'cognitive hacking'. The fourth article of our volume is dedicated to a precise description of this process. One of the countries that is highly digital and, at the same time, highly prone to possible Russian cyber or kinetic attacks is Estonia. The role of Estonia in providing Ukraine significant expertise in cyber defence is a topic of the fifth article of this special volume. Rest of the articles, that is sixth to tenth, in our volume are dedicated to more technical aspects of cybersecurity, such as digital tools of battlefield situational awareness, support of the EU for Ukraine cyber defence, or quantitative risk-based approach of network cyber defence. All articles in this special volume cover a wide range of topics pertinent to current political processes influenced by the Russian-Ukrainian conflict. We aim to contribute significantly to the understanding of political processes that are now stimulated by the Russian-Ukrainian conflict. The Editorial Board and I agree that democracy is currently facing its most substantial challenge after the end of World War II. It is imperative to enhance our understanding of the situation and the digital tools that adversaries used against democracies. Ukraine is enduring significant losses, including population displacement, infrastructure destruction, and paralysing cyberattacks. Despite these challenges, we believe that democracy will prevail, and the reconstruction of Ukraine will commence. This conflict has also strengthened cooperation among democratic countries, underscoring that unity and mutual support are crucial for overcoming contemporary military threats.

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Russia’s Cyber Campaigns and the Ukraine War: From the ‘Gray Zone’ to the ‘Red Zone’

Kristan Stoddart | Swansea University, UK | ORCID: 0000-0003-4996-6482

Received: 13.11.2023

Accepted: 20.05.2024

Published: 19.06.2024

Cite this article as:
K. Stoddart “Russia’s Cyber Campaigns and the Ukraine War: From the ‘Gray Zone’ to the ‘Red Zone’” ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/189358.

Corresponding author:
Kristan Stoddart, Swansea University, UK; E-Mail: K.D.Stoddart@Swansea.ac.uk
0000-0003-4996-6482

Abstract

This article examines Russia’s cyber campaigns against Ukraine and shines some light into this corner of the ‘gray zone’ and into the ‘red zone’ warfare inflicted upon Ukraine. Hitherto, there has been a lack of in-depth, systematic studies in relation to state-on-state cyber attacks. This article means to begin to bridge this gap in knowledge with its focus on Ukraine while arguing that Russia’s cyber campaigns are components of a wider suite of active measures/hybrid warfare engagements from its state and sub-state entities. For the Kremlin, hybrid warfare (*gibridnaya voina*) is fought with all the tools at their disposal on a ‘battlefield’ that stretches beyond the four modern domains of land, sea, air, and space. The fifth domain of cyberspace is increasingly important for espionage, cyberwar, and influence operations.

Keywords

Ukraine, Russia, hybrid, cyber, intelligence

1. Introduction: From the ‘Gray Zone’ to the ‘Red Zone’

This article outlines why on 24 February 2022 Russia invaded Ukraine under the pretext of military exercises. It demonstrates that the blunting of Russia’s cyber offensive against Ukraine that began in the months leading up to the invasion was potentially critical to the failure of Russia’s initial objectives and war aims [1]. According to a study by the Royal United Services Institute (RUSI), Russia expected to overrun Ukraine in a 10-day *blitzkrieg* [2].

Russia's *blitzkrieg* would be carried out by combat forces assembled for 'exercises' in the east of the Donbas oblast (region) as well as from northeast Donbas and northwest from occupied Crimea. They also formed a convoy south from Belarus where Russian forces had been conducting joint 'military exercises' [3–5].[1] Their aim from Belarus was to occupy Kyiv using their 12-1 conventional force advantage [2]. Sleeper agents, proxies, and collaborators (some inside Ukraine's own security service, the *Sluzhba bezpeky Ukrainy* [SBU]), who for years had been overstating their importance and influence, had told their Russian intelligence handlers (who paid them handsomely for their services) that Ukraine was weak and Russian forces would be welcomed as liberators [6, 7]. Part of this narrative is built on denials of Ukrainian statehood and references to a 'failed state' [8].

The Kremlin's battle plan underestimated Ukraine's abilities and will to resist, the aid they had been provided with (especially in cyber defences and real-time intelligence), while overestimating Russia's military preparedness combined with a deeply flawed and politicised series of intelligence assessments. These views are evidenced by literature from international relations, military think tanks, the cybersecurity industry, government sources as well as mainstream media reporting.

The Kremlin frames the war as a 'special military operation'. Kremlin propaganda insists its primary aims in Ukraine are to protect pro-Russian/Russian-speaking factions in Ukraine, especially in Crimea and the Donbas in Ukraine's east, and to 'de-nazify' and 'de-militarise' the country [9].[2] There are also background structural reasons. This includes a desire to challenge to the international liberal order, and to have a 'sphere of influence' over Ukraine [10, 11]. One *casus belli* has been North Atlantic Treaty Organization (NATO) enlargement, combined with Ukraine's decade-long drift since 2014 towards NATO and European Union (EU) membership [12–14]. If Putin's Russia wins or gains major concessions from Ukraine, this could have catastrophic consequences for NATO, the EU, and the international liberal order.

2. 'Colour Revolutions'

During the 1990s, Russia was at its weakest and unable to resist Western encroachment. For post-Cold War Russian

[1] There is evidence that the invasion was a last minute decision not communicated to field commanders until very late on and not communicated down the chain of command until after the decision had been made by Putin and a small inner circle of advisors [3–5].

[2] As Kuzio suggests, 'Soviet propaganda attacked Ukrainian nationalists with the "fascist" and "Nazi" label from the 1930s to the 1980s, terms that were revived by Putin's regime and President Yanukovych in the years leading to the Euromaidan. In Soviet and contemporary Russian eyes, a "fascist" is anyone who has turned their back on the USSR, Eurasian integration, and the Russian world" [9].

nationalists and political elites that were forming (or re-forming), this was viewed through the lens of the security dilemma and a zero-sum game [15]. This essentially structural realist view of international relations also contains heavy traces of Machiavellianism [16]. Since then, NATO/EU expansion has been portrayed as threatening politically, economically, and militarily to Russia's security and national interests. These elites see a security dilemma where the development of offensive and defensive capabilities becomes threatening, producing insecurity [17].[3] In the 1990s 'two-thirds of the Russian people, and … the majority of democratic politicians', viewed the dissolution 'as a tragic mistake, something that must somehow be undone' [18]. Putin was among them, and this bitterness has become a major driver for Russia's revanchist foreign and security policies.

For years prior to 2022, the design had been that as an independent state Ukraine would lean to Russia or be a pro-Russian proxy and not seek to join the EU or attempt accession to NATO [18].[4] In the intervening decade between the 2004 'Orange Revolution' and the 'Euromaidan' revolution in late 2013/early 2014, which deposed Ukraine's pro-Russian president Viktor Yanukovych, Ukraine had wrestled with divisions between Western reformist and Eastern *status quo* factions [19]. Euromaidan (and other 'Color Revolutions') were seen not as popular uprisings in the Kremlin but as 'foreign-sponsored regime changes' and security threats to Russia [20–22].[5]

Putin believed Euromaidan had been an orchestrated a coup by Western nations, particularly the United States and the Central Intelligence Agency (CIA), 'aimed at turning Ukraine into a barrier between Europe and Russia, a springboard against Russia', where 'radical nationalist groups [and neo-Nazis] served as its battering ram' [23]. In the interregnum between Yanukovych fleeing to Russia and his successor Petro Poroshenko being sworn in during the spring of 2014, Crimea was annexed [24]. Annexation utilised *Glavnoye Razvedovatel'noye Upravlenie* (GRU, Russian military intelligence) Spetsnaz special forces, who, stripped of insignia and blending in as local militia, became so-called 'Little Green Men', while political destabilisation and influence operations helped lay the groundwork for Russian ground forces [25]. Åtland argues this made it a 'blended conflict'; neither exclusively intrastate nor unambiguously interstate [26]. The Donbas conflict prior to February 2022 is also a good illustration of how Russia is adept at operations in the 'gray zone'; especially in creating plausible deniability over its use of armed force and intervention [5].

[3] The security dilemma is influenced by regime type, ethnocentrism, worst-case forecasting, and enemy imaging, among other things [17].

[4] Brzezinski provides a thoughtful perspective with modern-day repercussions [18].

[5] Putin himself commented in 2014 that 'There was a whole series of controlled "colour" revolutions. […] instead of democracy and freedom, there was chaos, outbreaks in violence and a series of upheavals. The Arab Spring turned into the Arab Winter. A similar situation unfolded in Ukraine' [21].

Russia stepped up support of the pro-Russian separatists in the Donbas after ‘Euromaidan’. As Crimea had experienced, destabilisation could be fermented from within and without through a mixture of mainstream and social media-driven propaganda, influence operations, lawfare (including passportisation of ‘pro-Russian’ Ukrainians), direct interventions, and Russian-inspired/directed military action [27]. This was designed to ferment secessionism and Russian nationalism in the self-declared Peoples Republics of Donetsk and Luhansk (DPR and LPR) [28]. This led to a ‘frozen conflict’ from 2014 to 2022 and thousands dying in the Donbas for little gain on either side [5].[6] Ukraine itself increasingly became a target for politico-military–economic reasons [29]. It was also being used to test the limits and responses to Russian actions, deployed widely across its near abroad, and in similar activities across four continents. Ukraine essentially became ‘a laboratory for Russian activities’ [30].

3. Russia’s Decade Long Use of Cyber: Debates over Cyberwarfare and the ‘Gray Zone’

Immediately prior to the invasion, the cyber side of Russia’s operations increased from Spring 2021 to Spring 2022. The targets included owner-operators of critical infrastructure (CI). Among the targets were municipal water suppliers as well as a major oil and gas company. In the weeks before February 2022, underground gas storage facilities, electricity operators, and healthcare providers were also specifically targeted along with agriculture and Internet service providers (ISPs) [31]. This could have been the first cyberwar (a vital modern component of hybrid warfare/active measures).[7]

However, what constitutes cyberwar/cyberwarfare is contested. It is often also misapplied to wider areas of cybersecurity, especially cyberespionage [32–34]. This is also because militaries are secondary players to intelligence agencies. A 2017 study of cyberwar(fare) definitions concluded that ‘a majority of articles do not offer explicit definitions of either cyber war or cyber warfare from which to base their analysis … characterised by both intra and interdisciplinary competition between dozens of definitions’ [32]. Richard Clarke, a former national security official and author of *Cyber War: The Next Threat to National Security and What to Do About It* and General Michael Hayden, a former NSA director, also recognise this definitional problem [35].

Others are skeptical of cyber war as a potential reality, given the absence of evidence [36–40]. This includes Joseph S. Nye, who

[6] This also reflects group think. Group think is described as ‘a result of the individuals involved being too similar in background (homogeneity) and not often enough in contact with alternative groups (insulation)’ [5].

[7] Active measures include propaganda, destabilization, forgery, assassination, acts of terrorism, hacking political parties, election interference, and dis/misinformation campaigns for political effect. Hybrid warfare can combine information, influence, agents of influence, legal disputes (lawfare), and economic operations as well as the use of military and paramilitary force and increasingly cyber operations.

wrote in 2018, ‘maybe we are looking in the wrong place, and the real danger is not major physical damage but conflict in the gray zone of hostility below the threshold of conventional warfare’ [41]. This line of reasoning is best summed up by Thomas Rid and his belief that ‘cyber war will not take place’. Rid centres his argument around three themes. First, cyberattacks are tools of non-violent sabotage. Second, cyberespionage decreases risk. Third, subversion decreases the resort to armed force. According to his line of argument, ‘cyberwar has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future’ [42].

4. Using Cyberespionage to Conduct Destructive and Debilitating Cyberwarfare

This article contests this view while recognising that these features are undoubtedly present. Orchestrated years long strategic campaigns of cyberespionage and sabotage can cross into destructive cyberwarfare. The two are intimately linked. Against Ukrainian CI, this could cross the threshold into attacks that could qualify as armed force under the UN Charter and NATO’s Tallinn Manuals/Process [43]. Energy infrastructure is a case in point where cyberespionage can pivot into destructive cyberwar with a direct threat to life and well-being.

It affects the physical world by maliciously altering the code of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Similarly, telecommunications, banking and transactions, transport as well as public utilities, such as energy and water, can be impacted. All sectors of CI rely on uninterrupted electricity supplies to function. Prior to and during the invasion, Russia has continually targeted CI facilities across multiple sectors. If they fail, Russia’s military has kinetically targeted key facilities with missile and drone strikes [44].

These are the most valuable cyber targets Ukraine has protected, because these service the civilian population and enable its military. Critical infrastructure facilities include not only ‘public utilities, such as electric power generation and distribution’, but ‘water supplies and water treatment, natural gas and oil production and pipelines, shipping and maritime traffic, hydroelectric dams, traffic lights, and train switching systems’ [43]. The most important sector of all to protect is electrical generation and distribution. Taking out electricity regionally or at-scale would have potentially blinded Ukraine, sent citizens into panic, and toppled the leadership. CI sites have become vulnerable because of growing connectivity, including through difficult to defend external Internet connections. Russia had demonstrated part of its capabilities before.

Russian cyberattacks began during the 2010s alongside 'other forms of cyber disruption and espionage to conduct a steady drumbeat of cyberattacks targeting Ukraine's government, military, telecommunications, and private sector information technology infrastructure' [45]. For years previously, Russia has been a determined user of cyberespionage for both intelligence gathering and 'preparation of the battlefield' in Ukraine, other parts of its near abroad, and in Western nations [46]. Highly targeted cyberattacks on Ukraine (and more widely) have been seen since 2014.

Russia's two main advanced persistent threat (APT) groups ('Fancy Bear'/APT28 and 'Cozy Bear'/APT29 run by the GRU and *Sluzhba Vneshnei Razvedki* [SVR, Russia's Foreign Intelligence Service], respectively) have been heavily involved [47, 48]. It is possible that 'Cozy Bear'/APT29 is run by Federal'naya Sluzhba Bezopasnosti (FSB, Federal Security Service), but there is good evidence the SVR is behind it [49]. In 2015 and again in 2016, 'Fancy Bear'/APT28 conducted cyberespionage campaigns (BlackEnergy and Industroyer/CrashOverride) that took out parts of Ukraine's regional grid system. This might well have been a direct response to events in kind which saw Ukraine cutting electricity supplies to Crimea in November 2015 [50]. Later, the Dutch and British governments attributed the BlackEnergy attacks to Russia's GRU and a team dubbed 'Sandworm' [51]. 'Sandworm' is linked to the GRU's Military Unit 74455 and has coordinated with APT28/'Fancy Bear' [52].

Through BlackEnergy, Ukraine became the first nation to experience a cyberattack, which took down part of its power grid (and arguably crossed the threshold into cyberwar). BlackEnergy evolved into a campaign spanning almost a decade and BlackEnergy 3.0 precision-targeted three regional power distribution companies leading to power cuts at Christmas 2015 [53]. While temporary, 225,000 customers were affected in Ukraine's Ivano-Frankivsk oblast [54]. The attack 'took multiple substations offline and disabled backup power from two distribution centers simultaneously' and automated telephone calls (robocalls) temporarily prevented customers from reporting outages. The attackers attempted to delay restoration by means of wiperware called KillDisk. The campaign likely took 'months of reconnaissance and planning' [55–57].

To place this in a wider context, if London had been the target, then as many as 1.45 million people could have been affected, and by attacking water sewerage systems (which rely on electricity), 3.9 million could have been affected [58]. These cyberattacks can also ‘look like preparations for future attacks that could be intended to harm Americans, or at least to deter the United States and other countries from protecting and defending our vital interests’, according to Admiral Mike Rogers [59]. Attacks on CI are far from exclusive to Ukraine and have included attempts on US power companies [43].

BlackEnergy was only the fourth ever known case of malicious code purpose-built to disrupt physical systems outside of computer laboratories. The first was Stuxnet, the second Shamoon, and the third a German steel mill. The next followed a year later. The malware, dubbed ‘Industroyer’ or ‘Crash Override’, was a major evolution of ‘the general-purpose tools’ used in 2015 [60]. It bore ‘many of the same technical hallmarks’ and was a demonstration of capability because Russia’s could have gone further [61–63]. The SBU again blamed the same Russian intelligence group [64]. ‘Industroyer’ caused a minor power outage in Kiev in December 2016. It was the culmination of a fortnight-long series of cyberattacks.

‘Industroyer’ could degrade power grids, scan and map ICS environments, and cause shutdowns to relays requiring a manual reset. Although it was designed to affect the electric grid in Ukraine, it can be re-engineered to affect multiple sectors of CI worldwide [65, 66]. It is not designed for espionage but to induce power outages (in this case, for a few days at worst). The attack was again attributed to the GRU’s ‘Sandworm’ group [67]. Development has not stood still with Industroyer 2.0 used in the Ukraine War [68].

In addition, Industroyer (and the KillDisk wiperware) was detected at Boryspil Airport in Kyiv, a mining company, and a railway company in Ukraine in 2016 [69]. At Boryspil, it could have affected air traffic control [70]. Bugdrop, another piece of sophisticated malware, was discovered in early 2017, predominantly in Ukraine, especially ‘in the self-declared separatist states of Donetsk and Luhansk’ [71]. It was designed to take screenshots as well as documents and passwords, and was able to eavesdrop on audio conversations by remotely controlling personal computer (PC) microphones. It was primarily used to target the energy sector [71]. In October 2017, BadRabbit ransomware disrupted Kyiv’s metro system and Odessa airport [51].

In 2018, a water treatment station at Auly, Dnipropetrovsk, was also hit by malware dubbed VPNFilter. This was prevented by

Ukraine's SBU. VPNFilter was capable of 'both cyber intelligence [gathering] and destructive cyber attacks' [72]. If successful, VPNFilter was configured to seize login credentials, exfiltrate data, monitor and reconfigure SCADA systems, and employ wiperware, which would have forced the plant offline. This wipes data from hard drives, which can only be recovered with great difficulty (if at all). The cybersecurity firm Talos identified 'overlaps with versions of the BlackEnergy malware' and went public with their assessments [73]. The US Department of Justice subsequently linked VPNFilter to 'Fancy Bear' [74].

This indicates the importance Russia accords critical infrastructure in Ukraine. Primary targets include energy and transport. The banking sector and Ukrainian elections have also been long-term targets [75, 76]. There is also evidence that Russia's GRU 'Fancy Bear' APT has previously used a 'trojan' (malware disguised as legitimate to infect a host) against Ukraine's military. This trojan, X-Agent (seen in campaigns elsewhere), infected an Android application developed by a Ukrainian military officer for use in artillery [77]. In July 2014, a successful Ukrainian offensive was blunted by a separatist counteroffensive with, it is alleged, support from Russian artillery (something Russian officials denied) because of X-Agent [78]. Russian cyber espionage in Ukraine also includes wiperware masquerading as cybercriminal ransomware attacks, most notably NotPetya in 2017 [79].

5. Cyberwarfare, Cyber defence, and Russia's Invasion

Immediately prior to the invasion in early February 2022, oil and port storage facilities across Europe were hit by cybercriminal ransomware gangs, dubbed BlackCat and Conti. Believed to be cybercrime, rather than state-sponsored, the attacks coincided with rising tensions and (well-founded) concerns in Europe over the disruption of energy supplies and wholesale price rises of oil and gas [80–83]. Despite Conti declaring its support of Russia and threatening further attacks on CI, the gang splintered because of internal divisions. They splintered further, as some members left Russia when conscripted to fight, while others chose to stay and continue to attack Ukraine [31].

Russia attempted cyberespionage and cyberwarfare against Ukraine immediately prior its invasion and during its early stages when it hoped to *blitzkrieg* the country. This was previously analysed in *Cyberwarfare: Threats to Critical Infrastructure* [43]. It included attacks on Viasat, a provider of satellite communications for commercial and military users, electrical substations in Ukraine (using an upgraded version of Industroyer/Crash Override), and Ukraine's railway network. Crucial support was provided by Western governments supported by private industry in preventing Russian cyberattacks, and crucial intelligence has been shared with Ukraine [43]. David Cattler, the assistant secretary general for intelligence and security at NATO, and Daniel Black, a principal analyst in the Cyber Threat Analysis Branch at NATO, wrote in *Foreign Affairs* in 2022:

> The belief that cyber-operations have played no role in Ukraine does not stem from a lack of real-world impact. To the contrary, the magnitude of Moscow's pre-kinetic destructive cyber-operations was unprecedented. On the day the invasion began, Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world's cyberpowers combined typically use in a given year [84].

Cattler and Black further caution that 'the lack of overwhelming "shock and awe" in cyberspace has led to the flawed presumption that Russia's cyber-units are incapable, and even worse, that cyber-operations have offered Russia no strategic value in its invasion of Ukraine' [84].

This line of analysis is supported by Microsoft, one of the key providers of support and cyber threat intelligence (CTI) to Ukraine [85].[8] Tom Burt, one of Microsoft's corporate vice presidents, disclosed that even before the invasion, they had been working around the clock to assist Ukraine. This included assisting government agencies against Russia's nation-state actors who had been engaging in full-scale offensive cyberwar. They had especially targeted Ukrainian CI [86]. This combined cyber and kinetic attacks on sites with the same geographic locations. Over 40% were CI sites, and 32% were Ukrainian government facilities [87]. This assessment was later upgraded to 55%, concentrating on energy, transportation, water, law enforcement, emergency services, and healthcare. This included attacking a Ukrainian energy ICS, where attempts were made to enter the operational technology (OT) side of operations. OT controls industrial processes and it is where cyberespionage pivots into destructive cyberwarfare [44].

[8] Through to 2023, Microsoft has given Ukraine more than $400 million in support. This 'unprecedented technology assistance' has included CI protection, the provision of cloud services as well as data and support to NGOs in relation to suspected war crimes and for humanitarian relief [85].

Specifically, Microsoft had detected new forms of offensive and destructive malware (including a trojan they dubbed ‘FoxBlade’) as part of renewed cyberattacks against Ukraine [88]. In total, Microsoft has detected at least nine wiperware variants, and two new types of ransomware. These have been used against over 100 Ukrainian private sector and government organisations. Additionally, at least 17 European nations have also experienced Russian cyberespionage attacks since the war began [89]. Wiperware has periodically knocked out power and water supplies across Ukraine.

Many of these attacks have been attributed to the GRU, combined with missile strikes against the same targets. These attacks were precisely targeted and included financial services, agriculture, emergency response services, humanitarian aid efforts as well as energy sector facilities. Microsoft’s president, Brad Smith, commented that as civilian targets they ‘raise serious concerns under the Geneva Convention, and we have shared information with the Ukrainian government about each of them’ [88].

From February 2023, a threat actor from the GRU was also mounting waves of cyberattacks against Ukrainian government agencies and IT service provides. It also targeted NATO member states assisting Ukraine. This included supply chains and logistics hubs in Poland [44]. This was the same GRU group that mounted the WhisperGate wiperware attacks first detected in January 2022 [43]. It is reported that this series of attacks was largely unsuccessful [90]. Figure 1 provides a good indicator of the range of cyberattacks that Russia has conducted.

Microsoft has regularly posted updates on the help they have provided as well as sharing intelligence on Russian activities. They indicated that as Winter 2022 turned into Summer 2023, Russia switched its seasonal focus to Ukraine’s agricultural sector. This saw Russia penetrate agribusinesses with malware, useful to steal data for intelligence and propaganda, alongside kinetic strikes. This caused damage to grain production that could have fed up to 1 million people for a year. This coincided with Russia’s withdrawal from the Black Sea Grain Initiative. As Summer 2023 turned to Winter 2023, Russia again turned its focus onto Ukraine’s energy infrastructure [92]. Both are breaches of the Law of Armed Conflict (LOAC). These and other charges have been levied by organisations, such as the International Criminal Court (ICC). When this has happened, Russian intelligence has attacked them as well as non-governmental organisations (NGOs) concerned with human rights [93].

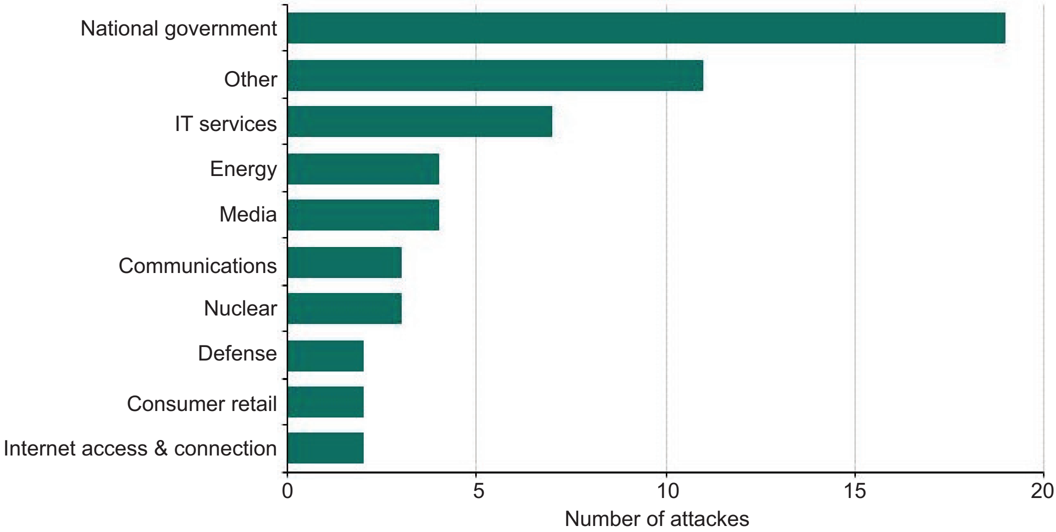


Figure 1. Cyber-attacks on Ukraine by Russia since the invasion began, by sector, July 2022. *Source*: https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine [91].

How many private cybersecurity providers have assisted Ukraine or offered their support is unclear. Those that have gone public include the industry giants Microsoft, Cisco Systems, and Amazon [94]. Although a number of providers have gone public, many might choose not to for various reasons, including concerns of reprisals. The support they provide could mean private corporations, like Microsoft, are considered by Russia and its proxies to be participants in the Russo-Ukraine War [95, 96].

Mandiant, ESET, and Recorded Future have also supplied services, tools, and CTI to Ukraine. Some of these have been procured through government contracts, others have provided *gratis* services. Their efforts helped secure networks and essential services and also prevented likely electricity blackouts [96]. According to Mandiant, 'this level of collective defense—between governments, companies, and security stakeholders across the world—is unprecedented in scope' [31]. These interventions, alongside those of Western governments and their intelligence agencies, were allied to those of Ukraine's State Services for Special Communication and Information Protection (SSSCIP), SBU, and civilian 'IT Army' of patriotic hackers [97]. Nevertheless, in the early months of the invasion, Ukraine also got 'very lucky' according to a senior official at SSSCIP [98].

They were also 'lucky' (as well as well prepared and well-resourced) when Russia targeted Ukraine's railway network in the Spring of 2022. 'Wiperware' was discovered *before* it was activated, but Russian intelligence APTs had penetrated its cyber defences. This too could have been critical. Ukraine's railways were a vital supply line inward for weapons and humanitarian aid and a lifeline for Ukrainian refugees fleeing the fighting. This could have had dire consequences. In the first 10 days of the war alone, 1 million Ukrainian civilians used it to flee to safety [99]. It was clear to NATO very early on that Russia would target CI [100].

Ukraine is facing specific state-level threats as well as attacks from Russia's own 'patriotic hacker' collectives. This includes the FSB's Center 16 (Military Unit 71330) and Center 18 (Unit 64829), SVR, and GRU and their 85th Main Special Service Center (GTsSS) in addition to their main centre for Special Technologies (GTsST/Unit 74455) as well as the Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM) of Russia's Ministry of Defense [101]. Between March and April 2022 high-voltage electrical substations in Ukraine were targeted by the 'Sandworm' group of Unit 74455. 'Sandworm' was deploying an upgraded version of Industroyer/Crash Override modular malware employed in 2016 (again alongside wiperware). As a precaution, nine electrical substations were temporarily switched off at a utility company servicing over 2 million people [98].

As Cattler and Black suggest,

> Russia's cyberattacks prior to the invasion suggest methodical preparations, with the attackers likely gaining access to Ukrainian networks months ago. This stands in stark contrast to the evident lack of preparation across Moscow's other military instruments, including on the ground, in the air, and in its frequently used influence operations through [mainstream] media and social media [84].

Lin similarly postulates that Russia's military might have had problems integrating their own cyber offensives with ground forces, especially given that a decision to invade might have been taken very late on and not well communicated down the chain of command [102].

Meanwhile, Russian forces have appeared more susceptible to interception than those in Ukraine. Electronic interception and jamming combined with deficient numbers of secure military communications equipment as well as the disorder of Russia's rank-and-file soldiers have been contributory factors [103]. Their personal cellphones and those stolen from Ukrainians have led to insecure communications on commercial networks. These have been intercepted and then leaked onto the Internet (including on Ukraine's SBU channel on YouTube). This provides significant and actionable real-time intelligence, including real-time geolocation and other metadata useful to Ukrainian forces. Additionally, Open Source Intelligence (OSINT) has been a feature of the conflict (and a rising feature of conflict, investigations, and accredited and citizen journalism more widely). For the Kremlin, this is a feature of the parallel information war they are waging with misinformation/disinformation and mal-information embedded into public political narratives and discourse. This is a feature of modern hybrid warfare [104, 105].

Their employment coincides with a spectrum of activities alongside conventional military force in the Russo-Ukraine War both in the run up to the invasion and during the war. It includes a series of cyber-enabled/cyber-enhanced overt and covert socio-political and economic pressure campaigns, as well as influence operations. This has leveraged agents of influence in Ukraine and beyond, cybercriminal gangs, and proxies, including the paramilitary Wagner Group.

While Elon Musk's Starlink satellite system has been important in maintaining Internet access (and Ukraine's resistance), Russia's military has found ways (including drones) to 'locate, jam, and degrade' the portable ground-based terminals 'which were never intended for battlefield use' [106]. Russian agencies have also been conducting renewed influence operations in an attempt to control (or cloud) the Kremlin's narrative at home and abroad. Microsoft's Brad Smith makes a highly pertinent observation in this respect. Smith postulates that just as Russia's APTs work within Russia's intelligence services, so do Advance Persistent Manipulator (APM) teams. These are not 'separate efforts' and we 'should not put them in separate analytical silos' [107].

6. Russia in 4D: Information Warfare at Home and Abroad

Influence operations are attempts to control politico-social narratives and for the Kremlin, they have become an increasingly important and highly cost-effective arm of foreign and security policy. They have been used to advance foreign and security policy aims to undermine Western states by influencing their electorates. Blowback has been minimised by censorship and prosecutions (or worse). Control of the information space has become central to Kremlin policy.

The importance that the Kremlin places on trying to control information cannot (and should not) be understated when examining Russia’s invasion of Ukraine. Tactical employment of dis-/mis- and mal-information has been utilised extensively by the Kremlin, not only in their approach to the war in Ukraine but also for managing political consent domestically [108–110]. This has seen them ‘wage a propaganda war’ [111]. Control over domestic media outlets and the distortion of facts are neither new nor uniquely Russian, but the Kremlin’s ‘narrative war’ against domestic opponents and Western critics has proven effective. These are part of the 4Ds of Russian information warfare: dismiss, distort, distract, and dismay. This dismisses critics, distorts facts, distracts from issues, and dismays the audience [112]. To these four needs to be added a fifth—disruption. This is not only in the domain of information warfare (*informatsionnaya voina*) but now, alongside a sixth D—destruction, needs setting in the context of hybrid warfare in Ukraine.

There is dismissal of even the use of the terminology of it being an invasion or a war. Instead, the Kremlin terms it a ‘special military operation’ (except on some rare occasions where Kremlin officials slip and war is referred to). The practice of Russia to dismiss any negative analysis or charges levied against either the Putin regime or Russian military has been a heavily used tactic by the Kremlin’s media machinery over the course of the invasion [113]. Disseminating ‘false information’ about Russia’s ‘special military operation’ has been criminalised in Russia. ‘Knowingly false information’ is redefined by amendments to Russia’s criminal code from information that is ‘objectively untrue’ to that which does not conform to ‘Russian official sources’ [114]. This has echoes of George Orwell’s novel *1984*. The dismissal of the reality in Ukraine is not confined to the inward-looking vector of media censorship.

The Kremlin has also employed both dismissal and distortion in their treatment of charges levied against them. Russia has regularly mentioned these as ‘smear campaigns’ staged by the West to ‘stoke Russophobia’ [115]. From at least 2014, the distortion of facts and evidence has been heavily employed. The most pertinent of these distortions are claims made on the prevalence of neo-Nazism in Ukrainian society and its military (particularly Ukraine’s Azov Brigade) [116]. Then there is the picture presented that President Zelenskyy had fallen ‘under the influence of radical elements’ [117]. In support of this distorted (mostly fictious) narrative, numerous fabricated or faked ‘evidence’ of military action have been reported and disseminated [118]. This has seen Russia suggest that atrocities it has been accused of are staged by Ukraine and the West [119].

This is why human rights NGOs have been targeted. Many other narratives were seeded related to Russia's invasion. Deepfake videos have also emerged [31]. This is being employed to mislead, confuse, distract, and interfere [120]. Its effect is greatest on the domestic population in Russia and maintaining support for a war whose losses have exceeded by far those experienced in Russia's 9-year occupation of Afghanistan (1979–1988) [121, 122].

Television is a particularly important source of information for most Russians. A longstanding trope utilises memories of World War II and Soviet/Russian patriotism to paint parts of Ukraine riven with Banderovtsy (followers of the Ukrainian nationalist Stepan Bandera during World War II). Distortion also occurs in reporting facts and events. This included evidence surrounding the shooting down of Malaysia Airlines flight MH17 by Russian-backed separatists in eastern Ukraine in July 2014. Calling out evidence and criticism as 'fake news' serves to dismiss and distract as well as seed doubts, leading to the distortion of reality. It is also where 'images are manipulated, fabricated or taken out of the context with the purpose of strengthening a false message' [123]. Distortion is widely used by the Kremlin.

To distract, a multitude of narratives and stories are continually seeded and disseminated about Ukraine and Western support. This is another hallmark of Russia's information war. Since 2014, the narratives regarding Ukraine and Ukrainian sovereignty have been chiming to regular drumbeats. Public policy pronouncements, speeches, television, and other mainstream media appearances (often simultaneously disseminated online) were inexhaustible in their frequency and falsehoods. For example, the sequence of events that led to flight MH17 being shot down was painted by Russia as everything from an attack committed by Ukraine to framing Russia (a false flag attack) to an evidence-less claim that all passengers were already dead and the plan was to explode the airliner over the Donbas as provocation [124].[9] This template was also used when the pro-war Russian military blogger Vladlen Tatarsky was assassinated with a statue containing a bomb in April 2023. The late Alexei Navalny's anti-corruption organisation was blamed, as was Ukrainian intelligence, and domestic terrorists [125].

This is template actively used against Ukraine, with unfounded claims, such as Ukraine is seeking radioactive 'dirty bombs' and bio-weapons. The scale of Russian disinformation campaigns was such that the EU founded the EUvsDisinfo project in 2015 to 'better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns'. Its database contains over 12,000

[9] On this single event, over 330 cases of pro-Kremlin disinformation have been identified [124].

samples; 40% relate to Ukraine [126, 127]. EUvsDisinfo centres this around '12 myths' which Paul and Matthews describe as a 'firehouse of falsehoods' churned out by Russia's propaganda machine. It is characterised by 'high number[s] of channels and messages and a shameless willingness to disseminate partial truths or outright fictions' [128]. This said, 'for all the propaganda on today's Kremlin-controlled television, the country remains far more open to information than in Soviet times' [129].

Russia also attempts to dismay domestic opposition and foreign audiences. The driving force behind much of these and other tactics of information warfare is not necessarily to make others believe their telling of events. It also weakens and undermines the West's ability to react decisively to geopolitical events concerning Russia as well as erode the confidence of Western populations in their respective governments and their policies towards Ukraine and Russia. As a former US Ambassador for Ukraine puts it: 'You could spend every hour of every day trying to bat down every lie … and that's exactly what the Kremlin wants' [130].

Until Western social media companies started to get a grip after 2016, this included the use, *en masse*, of trolls and automated botnets (bots) to sow and spread misinformation and disinformation on the Internet. These included 'false reports in genuine media outlets' which had measurable objectives and effects [131, 132]. These were (and still are) used by groups with false personas to tweet, like and post content in sync [133]. The most dangerous and destabilising use of dismaying messaging is through nuclear/weapons of mass destruction (WMD) saber rattling.

This rhetoric, repeated and amplified by serving and former members of government (including former President Dmitri Medvedev), and on Russian television by a cast list of (often vitriolic) nationalist commentators, has been a feature of the Russo-Ukraine War from its outset [134, 135]. These nuclear threats have also extended to civil nuclear power plants, such as Europe's largest in occupied Zaporizhzhia [136]. One of the earliest cases following the invasion sowed a claim that the United States was operating a series of biological weapon laboratories in Ukraine. This was reported on Russian state media and then rebroadcasted through self-described news organisations run by Russian intelligence onto Western social media platforms [31]. In December 2023, a Russian APM, dubbed Storm-1099, also attempted to spread misinformation that Ukrainian weapons were supplied to Hamas through the black market that were used in its 7 October 2023 attack on Israel [92].

For years, these tactics have been used to attack the democracies of Europe and the United States and undermine NATO. This has been directed by the Kremlin. Russia's intelligence, military, security services, media, public and private companies, organised criminal groups as well as social and religious organisations have all been involved. Dissent is not tolerated. They have spread malicious disinformation, engaged in election interference and political destabilisation campaigns (many far beyond Ukraine), and further fueled endemic internal corruption [137].

Through 'troll farms', it seeks to use the Internet, social media, and apps where information gets shared to spread state messaging. This state messaging includes official government statements, mainstream journalism (which almost always repeats or supports the official line or narrative) and (occasionally extreme) nationalist commentators. This framework helps 'create an alternative reality in which all truth is relative, and no information can be trusted' [112]. Parts of the narrative portrays the West, particularly the United States, as hostile to Russia with the EU and NATO threatening Russia's borders and negatively effecting Russia's 'sphere of influence' over the former Soviet states of its near abroad. Ukraine became the epicentre for these efforts after 'Euromaidan' in 2014, and through the lens of a security dilemma, Russia felt compelled to act [138].[10] The Kremlin has become adept at 'weaponising' information. It is also a part of *maskirovka*; a tactic of deception to mask, disguise, or camouflage (described by both Sun Tzu and Clausewitz) to serve politico-military ends [139].

7. Conclusion

Russia's invasion was the culmination of years of sustained and orchestrated pressure on Ukraine following 'Euromaidan' and the annexation of Crimea in 2014 [19, 140]. Western efforts in the winter of 2021 and spring of 2022 were critical to Ukraine's survival. It took a well-resourced and widespread series of (ongoing) efforts by Western governments/intelligence agencies and their cyber teams, combined with private industry to blunt these attacks. This effort support from Western multinationals such as Microsoft. Without it, Ukrainian defences could have been critically weakened, making it much harder to resist Russian military forces.

Against Ukraine, direct force has been employed *en masse* and this is more than asymmetric warfare. It is hybrid warfare beyond active measures employed previously [141]. Cyber is part of this for espionage, destructive warfare, and for information warfare and political

[10] Part of the Kremlin's rationale is that it finds itself in a security dilemma.

destabilisation. Escalating cyberattacks by Russia arguably began against Estonia in 2007, were used in Georgia in 2008, and have been used systematically against Ukraine since at least 2014. Thus far, these attacks have been resisted because of 'Kyiv's ability to harness the experience of years of Russian cyber attacks, combined with strong support from Western governments and—crucially—technology companies [and this] has allowed Ukraine to deploy cyber defenses at a scale and depth never seen before' [142].

This intervention recognises that 'cyber will now play an integral role in future armed conflict, supplementing traditional forms of warfare' [31]. At the same time, 'cyberwar' remains under-conceptualised, overused, and frequently conflated with wider cybersecurity issues, especially cyberespionage. While terminology remains ill-defined and contested, the boundaries and separation lead to confusion [143–145]. Information Warfare and the use of dis-information is another component of Russia's cyber offensive. This provides a good indicator of a multi-pronged strategy employed by Russia, consistent with Western conceptions of hybrid warfare and Russia's 'Gerasimov doctrine'. The resulting flair up of tensions in the Middle East also distracts from the Ukraine War [92].

In February 2022, it appears that the Kremlin saw an opportunity to step out of the 'gray zone' and enter the 'red zone' of war. Their war aims might change with events, but claiming victory through a negotiated settlement that includes Crimea and the Donbas could be another long peace or 20-year crisis [146, 147]. NATO and the EU are being tested. They cannot afford to fail that test. Prior to Russia's invasion, Mark Galeotti set this in a wider and more long-term context:

> Russia has reached back and re-learned a particular Soviet lesson, that political effects are what matters, not the means used to achieve them. Instead of trying to contest NATO where it is strongest, on the battlefield … it is instead an example of asymmetric warfare, using gamesmanship, corruption, and disinformation instead of direct force [148].

Russia's approach is not unique, but it goes further than other nations in trying to achieve its objectives. This strategy needs to be set in the context of 'Russia's long-standing, overall foreign policy objective … to weaken adversaries, particularly countries on its periphery, those in NATO, and the United States, by any means available' [131]. Across the West and into Africa's Sahel, they have been targeting nations unfriendly to the Kremlin or where Russia is seeking to grow its influence once more [149]. None more so than in Ukraine. How peace might manifest remains to be seen, but Russia's *modus operandi* under Putin is now long-established.

References

[1] D. Gioe, "Cyber operations and useful fools: the approach of Russian hybrid intelligence," *Intelligence and National Security,* vol. 33, no. 7, pp. 954–973, 2019, doi: 10.1080/02684527.2018.1479345.

[2] M. Zabrodskyi, J. Watling, O.V. Danylyuk, N. Reynolds, "Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February–July 2022," Nov. 2022. [Online]. Available: https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf. [Accessed Mar. 9, 2023].

[3] N. Masuhr, B. Zogg, "The War in Ukraine: First Lessons," Apr. 2022. [Online]. Available: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/540121/2/CSSAnalyse301-EN.pdf. [Accessed Mar. 9, 2023].

[4] J. Risen, (Mar. 11, 2022). *U.S. Intelligence says Putin made a last-minute decision to invade Ukraine*. [Online]. Available: https://theintercept.com/2022/03/11/russia-putin-ukraine-invasion-us-intelligence/. [Accessed Mar. 9, 2023].

[5] T. Bukkvoll, "Why Putin went to war: Ideology, interests and decision-making in the Russian use of force in Crimea and Donbas," *Contemporary Politics,* vol. 22, no. 3, pp. 273–279, 2016, doi: 10.1080/13569775.2016.1201310.

[6] M. Saito, M. Tsvetkova. (May 17, 2022). *The enemy within*. [Online]. Available: https://www.reuters.com/investigates/special-report/ukraine-crisisrussia-saboteurs/. [Accessed Apr. 11, 2023].

[7] M. Krever. (May 17, 2022). *Ukraine's security service hunts the spies selling information to Russia*. [Online]. Available: https://edition.cnn.com/2022/05/16/europe/ukraine-sbu-russian-spies-intl/index.html. [Accessed Apr. 11, 2023].

[8] T. Kuzio, *Russian Nationalism and the Russian-Ukrainian War*. Abingdon: Routledge, 2022.

[9] T. Kuzio, "European identity, Euromaidan, and Ukrainian nationalism," *Nationalism and Ethnic Politics,* vol. 22, no. 4, pp. 497–508, 2016, doi: 10.1080/13537113.2016.1238249.

[10] H. Suganami, "The causes of war," in *An Introduction to International Relations*, R. Devetak, A. Burke, J. George, Eds. Cambridge: Cambridge University Press, 3rd ed., 2017, pp. 225–234.

[11] K. Waltz, *Man, the State, and War: A theoretical Analysis Anniversary Edition*. New York: Columbia University Press, 2018.

[12] J.J. Mearsheimer, "Why the Ukraine crisis is the west's fault: The liberal delusions that provoked Putin," *Foreign Affairs,* vol. 93, no. 5, pp. 77–84, 2014.

[13] J.J. Mearsheimer, "The causes and consequences of the Ukraine War," *Horizons: Journal of International Relations and Sustainable Development*, vol. 21, no. 2, pp. 12–27, Summer 2022.

[14] N.R. Smith, G. Dawson, "Mearsheimer, Realism, and the Ukraine War," *Analyse & Kritik,* vol. 44, no. 2, pp. 175–200, 2022, doi: 10.1515/auk-2022-2023.

[15] G. Mangott, "Farewell to Russia: The decay of a superpower," in *Europe's New Security Challenges*, H. Gartner, A. Hyde-Price, E. Reiter, Eds., Boulder, CO: Lynne Rienner, 2001, pp. 381–385.

[16] S. Forde, "International realism and the science of politics: Thucydides, Machiavelli, and Neorealism," *International Studies Quarterly,* vol. 39, no. 2, pp. 141–160, 1995, doi: 10.2307/2600844.

[17] S. Tang, "The security dilemma: A conceptual analysis," *Security Studies,* vol. 18, no. 3, pp. 587–623, 2009, doi: 10.1080/09636410903133050.

[18] Z. Brzezinski, "The premature partnership," *Foreign Affairs,* vol. 73, no. 2, pp. 67–82, 1994, doi: 10.2307/20045920.

[19] L. Peisakhin, "Euromaidan revisited: Causes of regime change in Ukraine one year on," Wilson Center, Kennan Cable, no. 5, Feb. 2015. [Online]. Available: https://www.files.ethz.ch/isn/188792/5-kennan%20cable-Peisakhin.pdf. [Accessed Mar. 30, 2022].

[20] N. Bouchet, "Russia's 'militarization' of colour revolutions," *Policy Perspectives,* vol. 4, no. 2, pp. 1–2, 2016.

[21] V. Putin, (Mar. 18, 2014). *Address by President of the Russian Federation, 18 March, 15:50. The Kremlin, Moscow*. [Online]. Available: http://en.kremlin.ru/events/president/news/20603. [Accessed Apr. 24, 2024].

[22] M. Skak, "Russian strategic culture: The role of today's Chekisty," *Contemporary Politics,* vol. 22, no. 3, p. 324, 2016, doi: 10.1080/13569775.2016.1201317.

[23] V. Putin. (2022). *On the historical unity of Russians and Ukrainians*. [Online]. Available: en.kremlin.ru/events/president/news/66181. [Accessed: Apr. 3, 2022].

[24] J. Mankoff, "Russia's latest land grab: How Putin Won Crimea and Lost Ukraine," *Foreign Affairs,* vol. 93, no. 3, pp. 60–68, 2014.

[25] C.K. Bartles, R.N. McDermott, "Russia's military operation in Crimea road-testing rapid reaction capabilities," *Problems of Post-Communism,* vol. 61, no. 6, pp. 55–59, 2014.

[26] K. Åtland, "Destined for deadlock? Russia, Ukraine, and the unfulfilled Minsk agreements," *Post-Soviet Affairs,* vol. 36, no. 2, pp. 122–139, 2020, doi: 10.1080/1060586X.2020.1720443.

[27] F. Burkhardt, C. Wittke, E. Bescotti. (2022). *TCUP Report: Passportization, diminished citizenship rights, and the Donbas vote in Russia's 2021 Duma elections*. [Online]. Available: https://huri.harvard.edu/files/huri/files/idp_report_3_burkhardt_et_al.pdf?m=1642520438. [Accessed Mar. 21, 2023].

[28] J. Barbieri, "Raising citizen-soldiers in Donbas: Russia's role in promoting patriotic education programmes in the Donetsk and Luhansk Peoples' Republics" *Ethnopolitics,* forthcoming, 2023, doi: 10.1080/17449057.2023.2220097.

[29] K. Giles, "Russia and its neighbours: Old attitudes, new capabilities," in *Cyber War in Perspective: Russian Aggression against Ukraine,* K. Geers, Ed. Tallinn: NATO CCD COEPublications, 2015, pp. 19–28.

[30] A. Polyakova. (Mar. 22, 2018). *The next Russian attack will be far worse than bots and trolls*. [Online]. Available: https://www.brookings.edu/blog/orderfrom-chaos/2018/03/22/the-next-russian-attack-will-be-far-worse-than-botsand-trolls/amp/. [Accessed Sep. 30, 2019].

[31] Google's Threat Analysis Group (TAG), Mandiant, Google Trust & Safety. (2023). *Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape* [Online]. Available: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf. [Accessed Dec. 21, 2023].

[32] D. Hughes, A. Colarik, "The hierarchy of cyber war definitions," *Pacific Asia Workshop on Intelligence and Security*, 2017, doi: 10.1007/978-3-319-57463-9_2.

[33] K. Giles, W. Hagestad II, "Divided by a common language: Cyber definitions in Chinese, Russian and English," in *5th International Conference on Cyber Conflict Proceedings*, K. Podins, J. Stinissen, M. Maybaum, Eds., Tallinn: CCD COE Publications, 2013, pp. 413–430.

[34] S. D. Applegate, A. Stavrou, "Towards a cyber conflict taxonomy," in *5th International Conference on Cyber Conflict Proceedings*, K. Podins, J. Stinissen, M. Maybaum, Eds., Tallinn: CCD COE Publications, 2013, pp. 431–450.

[35] Washington Post Live. (Oct. 6, 2017). *Michael Hayden, Richard Clarke on greatest cyberthreats facing America*. [Online]. Available: https://www.youtube.com/watch?v=FdiAQBXGsMg. [Accessed Oct. 17, 2018].

[36] L. Kello, "The meaning of the cyber revolution perils to theory and statecraft," *International Security,* vol. 38, no. 2, pp. 9–14, 22, 2013, doi: 10.1162/ISEC_a_00138.

[37] D. Betz, "Cyberpower in strategic affairs: Neither unthinkable nor blessed," *Journal of Strategic Studies,* vol. 35, no. 5, pp. 689–711, 2012, doi: 10.1080/01402390.2012.706970.

[38] T. Junio, "How probable is cyber war? Bringing IR theory back into the cyber conflict debate," *Journal of Strategic Studies,* vol. 36, no. 1, pp. 125–133, 2013, doi: 10.1080/01402390.2012.739561.

[39] A.P. Liff, "The proliferation of cyberwarfare capabilities and interstate war, redux: Liff responds to Junio," *Journal of Strategic Studies,* vol. 36, no. 1, pp. 134–138, 2013, doi: 10.1080/01402390.2012.733312.

[40] E. Gartzke, "The myth of cyberwar bringing war in cyberspace back down to earth," *International Security,* vol. 38, no. 2, pp. 41–73, 2013, doi: 10.1162/ISEC_a_00136.

[41] J.S. Nye. (Jul. 5, 2018). *Is cyber the perfect weapon?* [Online]. Available: https://www.project-syndicate.org/commentary/deterring-cyber-attacks-and-information-warfare-by-joseph-s--nye-2018-07. [Accessed Sep. 13, 2018].

[42] T. Rid, *Cyber War Will Not Take Place*. London: Hurst, 2013.

[43] K. Stoddart, *Cyberwarfare: Threats to Critical Infrastructure*. London: Palgrave/Springer, 2022.

[44] C. Watts. (Dec. 3, 2022). *Preparing for a Russian cyber offensive against Ukraine this winter*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/. [Accessed Dec. 20, 2023].

[45] M. Connell, S. Vogler, *Russia's approach to cyber warfare, Occasional paper*, Center for Naval Analyses, 2017. [Online]. Available: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf. [Accessed Jan. 9, 2018].

[46] J. Weedon, "Beyond 'cyber war': Russia's use of strategic cyber espionage and information operations in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn: CCD COE Publications, 2015, pp. 67–77.

[47] Mitre Corporation, *APT28*. [Online]. Available: https://attack.mitre.org/groups/G0007/. [Accessed Jul. 19, 2023].

[48] Mitre Corporation, *APT29*. [Online]. Available: https://attack.mitre.org/groups/G0016/. [Accessed Jul. 19, 2023].

[49] H. Modderkolk, "Dutch agencies provide crucial intel about Russia's interference in US-elections," *De Volkskrant*, Jan. 25, 2018. [Online]. Available: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/. [Accessed Jul. 19, 2023].

[50] A. Osborn, P. Polityuk, "Russia prepares reprisals against Ukraine over Crimea blackout," *Reuters*, Nov. 24, 2015. [Online]. Available: https://www.reuters.com/article/us-ukraine-crisis-crimea-idUSKBN0TD1NI20151124. [Accessed Feb. 28, 2020].

[51] National Cyber Security Centre. (Oct. 4, 2018). *Reckless campaign of cyber attacks by Russian military intelligence service exposed*. [Online]. Available: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russianmilitary-intelligence-service-exposed. [Accessed Jan. 10, 2019].

[52] A. Greenberg, "Hackers tied to Russia's GRU targeted the US grid for years, researchers warn," *Wired*, Feb. 24, 2021. [Online]. Available: https://www.wired.com/story/russia-gru-hackers-us-grid/. [Accessed Apr. 11, 2023].

[53] N. Zinets, "Ukraine charges Russia with new cyber attacks on infrastructure," *Reuters*, Feb. 15, 2017. [Online]. Available: http://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-charges-russia-with-new-cyber-attacks-on-infrastructure-idUSKBN15U2CN. [Accessed Sep. 7, 2017].

[54] CISA. (Jul. 20, 2021). *ICS alert cyber-attack against Ukrainian critical infrastructure*. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [Accessed Dec. 28, 2023].

[55] Idaho National Laboratory. (2016). *Cyber threat and vulnerability analysis of the U.S. electric sector prepared by: Mission support center*. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf. [Accessed Aug. 12, 2019].

[56] ICS/SANS. (Mar. 18, 2016). *TLP: White analysis of the cyber attack on the Ukrainian power grid defense use case*. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. [Accessed Jan. 19, 2018].

[57] P. Polityuk, "Ukraine to probe suspected Russian cyber attack on grid," *Reuters*, Dec. 31, 2015. [Online]. Available: https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231?feedType=RSS. [Accessed Jan. 19, 2018].

[58] E.J. Oughton, D. Ralph, R. Pant, E. Leverett, J. Copic, et al., "Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks

on electricity distribution infrastructure networks," *Risk Analysis,* vol. 39, no. 9, pp. 2012–2031, 2019, doi: 10.1111/risa.13291.

[59] C-Span. (May 9, 2017). *Cybersecurity threats and defense strategy*. [Online]. Available: https://www.c-span.org/video/?428023-1/cybersecurity-threats-defense strategy&start=1166. [Accessed Sep. 27, 2018].

[60] D. Goodin. (Jun. 12, 2017). *Found: 'Crash override' malware that triggered Ukrainian power outage attack tools can be used against a broad range of electric grids around the world*. [Online]. Available: https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotageelectric-grids-but-its-no-stuxnet/. [Accessed Jan. 20, 2018].

[61] D. Goodin. (Jan. 11, 2017). *Hackers trigger yet another power outage in Ukraine for the second year in a row, hack targets Ukraine during one of its coldest months*. [Online]. Available: https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hitsukraine/. [Accessed Jan. 19, 2018].

[62] ESET. (Jun. 12, 2017). *Industroyer: Biggest malware threat to critical infrastructure since Stuxnet*. [Online]. Available: https://www.eset.com/int/industroyer/. [Accessed Jan. 19, 2018].

[63] US-CERT. (Jul. 27, 2017). *Alert (TA17-163A) crash override malware*. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-163A. [Accessed Jan. 19, 2018].

[64] P. Polityuk, "Ukraine points finger at Russian security services in recent cyber attack," *Reuters*, Jul. 1, 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P. [Accessed Jan. 19, 2018].

[65] US-CERT. (Jul. 27, 2017). *Alert (TA17-163A) crash override malware*. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-163A. [Accessed Jan. 19, 2018].

[66] ESET. (Jun. 12, 2017). *Industroyer: Biggest malware threat to critical infrastructure since Stuxnet*. [Online]. Available: https://www.eset.com/int/industroyer/. [Accessed Jan. 19, 2018].

[67] Dragos. (2017). *Crashoverride analysis of the threat to electric grid operations.* [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf. [Accessed Oct. 7, 2018].

[68] Mandiant. (2023). *M-trends 2023*. [Online]. Available: https://services.google.com/fh/files/misc/m_trends_2023_report.pdf. [Accessed Dec. 21, 2023].

[69] Trend Micro. (Jun. 28, 2016). *Cyber threats to the mining industry*. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/cyber-threats-to-the-mining-industry. [Accessed Mar. 27, 2023].

[70] M. Baezner, *Cyber and information warfare in the Ukrainian conflict, Center for Security Studies, ETH Zurich, Oct. 2018*. [Online]. Available: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/321570/20181003_MB_HS_RUS-UKRV2_rev.pdf?sequence=1. [Accessed Mar. 27,2023].

[71] CybrerX Labs. (Feb. 15, 2017). *Operation BugDrop: CyberX discovers large-scale cyber-reconnaissance operation targeting Ukrainian organizations*. [Online].

Available: https://cyberx-labs.com/blog/operation-bugdrop-cyberx-discoverslarge-scale-cyber-reconnaissance-operation/. [Accessed Dec. 16, 2018].

[72] Interfax. (Jul. 11, 2018). *SBU thwarts cyber attack from Russia against chlorine station in Dnipropetrovsk region*. [Online]. Available: https://en.interfax.com.ua/news/general/517337.html. [Accessed Mar. 27, 2023].

[73] W. Largent.(May 23, 2018). *New VPNFilter malware targets at least 500K networking devices worldwide*. [Online]. Available: https://blog.talosintelligence.com/vpnfilter/. [Accessed Mar. 27, 2023].

[74] US Department of Justice. (May 23, 2018). *Justice Department announces actions to disrupt advanced persistent threat 28 Botnet of infected routers and network storage devices.* [Online]. Available: https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistentthreat-28-botnet-infected. [Accessed Mar. 27, 2023].

[75] A. Greenberg, "Everything we know about Russia's election-hacking playbook," *Wired*, Jun. 9, 2017. [Online]. Available: https://www.wired.com/story/russia-election-hacking-playbook/. [Accessed Mar. 27, 2023].

[76] P. Polityuk, "Exclusive: Ukraine says it sees surge in cyber attacks targeting election," *Reuters*, Jan. 25, 2019. [Online]. Available: https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX. [Accessed Mar. 27, 2023].

[77] A. Meyers, "Danger Close: Fancy bear tracking of Ukrainian field artillery units," *Crowdstrike*, Dec. 22, 2016. [Online]. Available: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. [Accessed Mar. 27, 2023].

[78] Bellingcat. (Feb. 17, 2015). *Bellingcat report—Origin of artillery attacks on Ukrainian military positions in Eastern Ukraine between 14 July 2014 and 8 August 2014.* [Online]. Available: https://www.bellingcat.com/news/uk-andeurope/2015/02/17/origin-of-artillery-attacks/. [Accessed Mar. 27, 2023].

[79] US Department of Justice. (2015). *Press release*. [Online]. Available: https://www.justice.gov/opa/press-release/file/1328521/download. [Accessed Mar. 27, 2023].

[80] Microsoft. (Jan. 15, 2022). *Destructive malware targeting Ukrainian organizations.* [Online]. Available: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.[Accessed May 20, 2022].

[81] J. Tidy. (Feb. 3, 2022). *European oil facilities hit by cyber-attacks*. [Online]. Available: https://www.bbc.co.uk/news/technology-60250956. [Accessed May 20, 2022].

[82] A. Ribeiro. (Feb. 4, 2022). *Cyberattacks continue to extend across Europe, BlackCat ransomware may be involved.* [Online]. Available: https://industrialcyber.co/threats-attacks/cyberattacks-continue-to-extend-acrosseurope-blackcat-ransomware-may-be-involved/. [Accessed May 20, 2022].

[83] M. Wigell, A. Vihma, "Geopolitics versus geoeconomics: The case of Russia's geostrategy and its effects on the EU," *International Affairs,* vol. 92, no. 3, pp. 605–627, 2016, doi: 10.1111/1468-2346.12600.

[84] D. Cattler, D. Black, "The myth of the missing cyberwar," *Foreign Affairs*, Apr. 6, 2022. [Online]. Available: www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar. [Accessed Apr. 11, 2023].

[85] B. Smith. (Nov 3, 2022). *Extending our vital technology support for Ukraine.* [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/11/03/ourtech-support-ukraine/. [Accessed Dec. 18, 2023].

[86] Microsoft. (Apr. 7, 2022). *Disrupting cyberattacks targeting Ukraine*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattack-sukraine-strontium-russia/. [Accessed May 19, 2022].

[87] Microsoft. (Apr. 27, 2022). *Special report: Ukraine an overview of Russia's cyberattack activity in Ukraine*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. [Accessed Apr. 11, 2023].

[88] Microsoft. (Feb. 28, 2022). *Digital technology and the war in Ukraine*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine russia-digital-war-cyberattacks/. [Accessed May 19, 2022].

[89] C. Watts.(Mar 15, 2023). *Is Russia regrouping for renewed cyberwar?* [Online]. Available: https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/. [Accessed Dec 20, 2023].

[90] T. Burt. (Jun 14, 2023). *Ongoing Russian cyberattacks targeting Ukraine.*[Online]. Available: https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyber attacks-ukraine-cadet-blizzard/. [Accessed Dec. 20, 2023].

[91] Office for Budgetary Responsibility. (2022). *Cyber-attacks on Ukraine by Russia since the invasion began, by sector*. [Online]. Available: https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/. [Accessed Dec. 19, 2023].

[92] C. Watts. (Dec. 7, 2023). *Russian influence and cyber operations adapt for long haul and exploit war fatigue.* [Online]. Available: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebritycameo-mtac/. [Accessed Dec. 20, 2023].

[93] F.R. Partipilo, M. Stroppa, "Humanitarian organisations under cyber-attack," in *Responsible Behaviour in Cyberspace: Global Narratives and Practice*, A. Sukumar, D. Broeders, F. Delerue, Eds., Gilly, Beitlot/Luxembourg: Publications Office of the European Union, 2023, pp. 238–257.

[94] N. Biasini, M. Chen, A. Karkins, A. Khodjibaev, C. Neal, M. Olney, D. Korzhevin. (Jan. 21, 2022.). *Ukraine campaign delivers defacement and wipers, in continued escalation*. [Online]. Available: https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html. [Accessed May 21, 2022].

[95] M. Hill. (Mar. 2, 2022). *How security vendors are aiding Ukraine*. [Online]. Available: https://www.csoonline.com/article/3651685/how-security-vendorsare-aiding-ukraine.html. [Accessed Dec. 17, 2023].

[96] K. Zetter, (Dec. 7, 2022). *Security firms aiding Ukraine during war could be considered participants in conflict*. [Online]. Available: https://www.zetter-zeroday.com/p/security-firms-aiding-ukraine-during. [Accessed Dec. 17, 2023].

[97] S. Schechner, "Ukraine's 'IT army' has hundreds of thousands of hackers, Kyiv says," *The Wall Street Journal*, Mar. 4, 2022. [Online]. Available: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX. [Accessed: May 20, 2022].

[98] A. Greenberg, “Russia’s sandworm hackers attempted a third blackout in Ukraine,” *Wired*, Apr. 12, 2022. [Online]. Available: https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/. [Accessed: Dec. 28, 2023].

[99] C. Krebbs, “The cyber warfare predicted in Ukraine may be yet to come,” *Financial Times*, Mar. 20, 2022. [Online]. Available: https://www.ft.com/content/2938a3cd-1825-4013-8219-4ee6342e20ca. [Accessed: May 21, 2022].

[100] CCDCOE. (2022). *World’s largest international live-fire cyber exercise launches in Tallinn*. [Online]. Available: https://ccdcoe.org/news/2022/lockedshields-2022-exercise-to-be-launched-next-week/. [Accessed: May 21, 2022].

[101] CISA. (Apr. 20, 2022). *Joint cybersecurity advisory Russian state-sponsored and criminal cyber threats to critical infrastructure*. [Online]. Available: https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf. [Accessed: May 19, 2022].

[102] H. Lin, “Russian cyber operations in the invasion of Ukraine,” *Cyber Defense Review,* vol. 7, no. 4, pp. 37–38, 2022.

[103] D. Ong, “Russian general brutally dies in Ukraine: ‘Collected his guts…back in his belly’,” *International Business Times*, Apr. 27, 2022. [Online]. Available: https://www.ibtimes.com/russian-general-brutally-dies-ukraine-collected-his-gutsback-his-belly-3488076. [Accessed: May 23, 2022].

[104] J. Grady. (Mar. 18, 2022). I*ntel sharing between U.S. and Ukraine ‘Revolutionary’ says DIA Director*. [Online]. Available: https://news.usni.org/2022/03/18/intel-sharing-between-u-s-and-ukraine-revolutionary-says-dia-director. [Accessed: May 22, 2022].

[105] N.S. Abdalla, P. H.J. Davies, K. Gustafson, D. Lomas, S. Wagner, “Intelligence and the War in Ukraine,” *War on the Rocks*, May 11, 2022. [Online]. Available: Part 1: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/, Part 2: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/. [Accessed: May 22, 2022].

[106] S. Skove, “Using starlink paints a target on Ukrainian troops,” *Defense One*, Mar. 23, 2023. [Online]. Available: https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/. [Accessed: Mar 25, 2023].

[107] B. Smith, “Defending Ukraine: Early lessons from the cyber war,” *Microsoft On the Issues*, Jun 22, 2022. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. [Accessed: Jun 23, 2022].

[108] R. Smith, *Elections, Protest, and Authoritarian Regime Stability: Russia 2008–2020*. Cambridge: Cambridge University Press, 2020.

[109] R. Smith, “Vladimir Putin plans to win Russia’s parliamentary election no matter how unpopular his party is,” *The Conversation*, Aug. 16, 2021. [Online]. Available: https://theconversation.com/vladimir-putin-plans-to-win-russias-parliamentary-election-no-matter-how-unpopular-his-party-is-160078. [Accessed: Jun 18, 2023].

[110] S. Herman, N. Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*. London: Vintage Books, 1994.

[111] R. DiResta, K. Shaffer, B. Ruppel, D. Sullivan, R. Matney, R. Fox, “The Tactics and Tropes of the Internet Research Agency,” *New Knowledge*, Dec. 17, 2018.

[Online]. Available: https://archive.org/details/5635464-NewKnowledge-Disinformation-Report-Whitepaper/mode/2up. [Accessed: Aug. 26, 2019].

[112] B. Nimmo, "Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it," *StopFake*, May 19, 2015. [Online]. Available: https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/. [Accessed: Apr. 2, 2023].

[113] *Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities – Consilium*, Consilium, Jul. 28, 2023. [Online]. Available: https://www.consilium.europa.eu/en/press/pressreleases/2023/07/28/information-manipulation-in-russia-s-war-of-aggressionagainst-ukraine-eu-lists-seven-individuals-and-five-entities/. [Accessed: Jul. 30, 2023].

[114] Committee to Protect Journalists. (2022). *Understanding the laws relating to 'fake news' in Russia*. [Online]. Available: https://cpj.org/wp-content/uploads/2022/07/Guide-to-Understanding-the-Laws-Relating-to-Fake-News-in-Russia.pdf. [Accessed: Mar. 25, 2023].

[115] G. Faulconbridge, T. Janowski. (Apr. 11, 2022). *Russia says West helping Ukraine prepare fake allegations of war crimes*. [Online]. Available: https://www.reuters.com/world/europe/russia-says-west-helping-ukraine-prepare-fakeallegations-war-crimes-2022-04-11/. [Accessed: Mar. 25, 2023].

[116] I. Gaber, "Believing what they are told," *British Journalism Review*, vol. 33, no. 3, pp. 22-26, 2022, doi: 10.1177/09564748221121469.

[117] Tass. (Dec. 23, 2021). *Zelensky under the influence of radical elements, says Putin*. [Online]. Available: https://tass.com/politics/1380001. [Accessed: Mar. 26, 2023].

[118] M. Trobridge. (Apr. 13, 2022). *Fact check: How to spot a fake military success story.* [Online]. Available: https://www.dw.com/en/fact-check-how-to-spot-afake-military-success-story-in-russia-ukraine-war/a-61453500. [Accessed: Mar. 25, 2023].

[119] O. Dudko, "A conceptual limbo of genocide: Russian rhetoric, mass atrocities in Ukraine, and the current definition's limits," *Canadian Slavonic Papers,* vol. 64, no. 2–3, pp. 133–145, 2022, doi: 10.1080/00085006.2022.2106691.

[120] T.C. Shea, "Post-Soviet Maskirovka, cold war nostalgia, and peacetime engagement," *Military Review,* vol. 82, no. 3, pp. 63–67, 2022.

[121] J. Landay, "U.S. intelligence assesses Ukraine war has cost Russia 315,000 casualties – source," *Reuters*, Dec. 12, 2023. [Online]. Available: https://www.reuters.com/world/us-intelligence-assesses-ukraine-war-has-cost-russia-315000-casualties-source-2023-12-12/. [Accessed: Dec 2023].

[122] I. Garner, "We've got to kill them": Responses to Bucha on Russian social media groups," *Journal of Genocide Research,* vol. 25, Issue 3–4, pp. 41–8–425, 2023, doi: 10.1080/14623528.2022.2074020.

[123] I. Khaldarova, M. Pantti, "Fake News: The narrative battle over the Ukrainian conflict," *Journalism Practice,* vol. 10, no. 7, pp. 891–901, 2016, doi: 10.1080/17512786.2016.1163237.

[124] EUvsDisinfo. (Nov. 24, 2022). *Throwing mud at everyone and hoping some of it sticks*. [Online]. Available: https://euvsdisinfo.eu/throwing-mud-at-everyone-and-hoping-some-of-it-sticks/?highlight=mh17. [Accessed: Mar. 26, 2023].

[125] K. Stepanenko, F.W. Kagan. (Apr. 2, 2023). *Russian offensive campaign assessment, Institute for the Study of War*. [Online]. Available: https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-2-2023. [Accessed: Apr. 6, 2023].

[126] EUvsDisinfo. *About*. [Online]. Available: https://euvsdisinfo.eu/about/. [Accessed: Mar. 26, 2023].

[127] EUvsDisinfo. *Ukraine*. [Online]. Available: https://euvsdisinfo.eu/ukraine/. [Accessed: Mar. 26, 2023].

[128] C. Paul, M. Matthews. (2016). *The Russian 'firehose of falsehood' propaganda model, RAND Corporation*. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf. [Accessed: Mar. 26, 2023].

[129] D. Treisman, Ed., *The New Autocracy: Information, Politics, and Policy in Putin's Russia.* Washington DC: Brookings Institution Press, 2018.

[130] Business Ukraine. (Dec. 5, 2015). *Interview: U.S. Ambassador Geoffrey Pyatt on Euromaidan, Ukrainian reforms and Kremlin trolls*. [Online]. Available: http://bunews.com.ua/interviews/item/interview-us-ambassador-geoffrey-pyatt-oneuromaidan-ukrainian-reforms-and-kremlin-trolls. [Accessed: Apr. 3, 2023].

[131] K. Giles, "Countering Russian information operations in the age of social media," *Council on Foreign Relations*, Nov. 21, 2017. [Online]. Available: https://www.cfr.org/report/countering-russian-information-operations-age-social-media. [Accessed: Oct. 25, 2019].

[132] BBC News. (Nov. 14, 2017). *How Russian bots appear in your timeline*. [Online]. Available: https://www.bbc.co.uk/news/technology-41982569. [Accessed: Oct. 25, 2019].

[133] B. Abeshouse, "Troll factories, bots and fake news: Inside the Wild West of social media," *Al Jazeera*, Feb. 8, 2018. [Online]. Available: https://www.aljazeera.com/blogs/americas/2018/02/troll-factories-bots-fake-news-wild-west-social-media-180207061815575.html. [Accessed: Nov. 12, 2019].

[134] United Nations. (Aug. 22, 2022). *'Nuclear Sabre-rattling must stop,' Secretary-General tells Security Council, calling on States to ease tensions, end atomic weapons race*, United Nations Press Release. [Online]. Available: https://press.un.org/en/2022/sc15001.doc.htm. [Accessed: Apr. 6, 2023].

[135] M. Budjeryn. (Nov. 9, 2022). *Distressing a system in distress: Global nuclear order and Russia's war against Ukraine*. [Online]. Available: https://thebulletin.org/premium/2022-11/distressing-a-system-in-distress-global-nuclearorder-and-russias-war-against-ukraine/#post-heading. [Accessed: Apr. 6, 2023].

[136] R.C. Ewing, "Nuclear reactors in a war zone: A new type of weapon?," *Bulletin of the Atomic Scientists*, Mar. 7, 2022. [Online]. Available: https://thebulletin.org/2022/03/nuclear-reactors-in-a-war-zone-a-new-type-of-weapon/#post-heading. [Accessed: Apr. 6, 2023].

[137] Committee on Foreign Relations, United States Senate. (Jan. 10, 2018). *Putin's asymmetric assault on democracy in Russia and Europe: Implications for U.S. national security a minority staff report.* [Online]. Available: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf. [Accessed: Nov. 5, 2019].

[138] D. Averre, "The Ukraine Conflict: Russia's challenge to European security governance," *Europe-Asia Studies,* vol. 68, no. 4, pp. 699–725, 2016, doi: 10.1080/09668136.2016.1176993.

[139] D.W. Kruger. (Dec. 4, 1987). *Maskirovka – What's In It for Us?, Fort Leavenworth, KS: School of Advanced Military Studies*. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a190836.pdf. [Accessed: Jan. 13, 2019].

[140] T. Kuzio, "Ukraine's Orange Revolution, the oppositions road to success," *Journal of Democracy,* vol. 16, no. 2, pp. 117–130, 2005, doi: 10.1353/jod.2005.0028.

[141] A. Racks. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. Helsinki: Finnish Institute of International Affairs (FII).* [Online]. Available: http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/. [Accessed: Jan. 13, 2019].

[142] J. Bateman, N. Beecroft, G. Wilde, *What the Russian Invasion Reveals About the Future of Cyber Warfare*. Washington, DC: Carnegie Endowment for International Peace, Dec. 19, 2022. [Online]. Available: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667. [Accessed: Dec. 18, 2023].

[143] J. Goldsmith, "How cyber changes the laws of war," *European Journal of International Law,* vol. 24, no. 1, pp. 129–138, 2013, doi: 10.1093/ejil/cht004.

[144] M. Robinson, K. Jones, H. Janicke, "Cyber Warfare: Issues and Challenges," *Computers & Security*, vol. 49, pp. 70–94, 2015, doi: 10.1016/j.cose.2014.11.007.

[145] M.C. Libicki, "Cyberspace is not a warfighting domain," *Journal of Law and Policy for the Information Society,* vol. 8, no. 2, pp. 325–340, 2012.

[146] P. Cunliffe, *The New Twenty Years' Crisis: 1999–2019*. Montreal: McGill-Queens University Press, 2020.

[147] J.L. Gaddis, "International relations theory and the end of the Cold War," *International Security,* vol. 17, no. 3, pp. 5–58, 1992–1993, doi: 10.2307/2539129.

[148] M. Galeotti, "(Mis)understanding Russia's two 'hybrid wars'," *Critique & Humanism*, vol. 59, no. 1, p. 5, 2018. Reprinted in *Eurozine*. Available: https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/?pdf.

[149] House of Commons Foreign Affairs Committee. (Jul. 18, 2023). *Guns for gold: The Wagner Network exposed, Seventh Report of Session 2022–23.* [Online]. Available: https://committees.parliament.uk/publications/41073/documents/200048/default/. [Accessed: Jul. 26, 2023].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Moscow and the World: From Soviet Active Measures to Russian Information Warfare

Roger E. Kanet | University of Miami, USA, ORCID: 0000-0002-2041-9429

Received: 9.12.2023

Accepted: 7.02.2024

Published: 18.04.2024

Cite this article as:
R.E. Kanet "Moscow and the World: From Soviet Active Measures to Russian Information Warfare," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/162742.

Corresponding author:
Roger E. Kanet, University of Miami, USA;
0000-0002-2041-9429

Abstract

Russia under Vladimir Putin has expanded and moved rapidly to improve its ability to employ "disinformation," or "information warfare," as an effective instrument to help it to accomplish its specific foreign policy objectives. Although it has only been since direct Russian involvement in the U.S. presidential election of 2016 that this has been an issue of major public political concern in the United States, a flood of research on this topic has now begun to appear. Despite many years of preparation for cyber conflict against critical U.S. infrastructure and military forces, the U.S. government and cybersecurity industry were unprepared for Russian information operations targeting the 2016 U.S. presidential election. It is clear, however, that the Russian propaganda/ disinformation activities in the U.S. are but one part of a policy targeted virtually everywhere across the entire world and that this policy builds upon the earlier propaganda and disinformation activities of Russia's predecessor state, the USSR. In the present essay, we intend to track the reemergence and development of the information warfare and disinformation component of Russian policy under President Putin, including its largely successful attempt to reintegrate the components of the former Soviet Union and its deep roots in Soviet "active measures," up until the invasion of Ukraine, when it expanded exponentially. We shall also track the areas of the world targeted, and the increasing breadth of its target audiences and the issues covered.

Keywords

disinformation warfare, propaganda, Russia, USSR

1. Soviet Propaganda and Disinformation Policy[1]

Current Russian disinformation policy clearly has its roots in what the Soviets termed "active measures" and in which they included both propaganda and disinformation. On the propaganda side, for example, in 1983, the Soviets published books in eighty-four foreign languages mainly for distribution abroad. In English alone 1,200 books and pamphlets appeared in more than 24 million copies [4]. The weekly *Moscow News* appeared in more than 800,000 copies in English, French, Spanish, and Arabic translations at that time [5]. Besides direct dissemination of Soviet propaganda, the Soviets also relied on the wide network of foreign communist and front organisations to distribute Soviet-oriented propaganda.

The purpose of this propaganda network and facilities was to support both general and specific Soviet foreign policy objectives–more specifically to weaken the United States and North Atlantic Treaty Organization (NATO) and to extoll the achievements of the USSR, thereby advancing Moscow's objectives. The definition of propaganda used in this analysis is based on that developed by Hazan [6] as a preconceived, systematic and centrally coordinated process of manipulating symbols, aimed at promoting certain uniform attitudes, beliefs, values, and behaviour within mass audiences abroad – these expected attitudes, beliefs, values and behaviour are congruent with the specific interests and ends of the propagandist.[2]

Related to, but distinct from propaganda, is disinformation, defined as any governmental-sponsored communication of intentionally false and misleading material (often combined with selectively true information) which is passed to targeted individuals, groups, or governments with the purposes of influencing foreign elite or public opinion and policies [8]; see also [9]. Propaganda differs from disinformation in two important ways. The former is targeted at a mass audience and is not necessarily deceptive, while disinformation is aimed ultimately at foreign policy decision makers and is always purposefully deceptive.

Propaganda and disinformation belong to a category of activities, which the Soviets referred to as "active measures," including both overt and covert techniques employed for the purpose of influencing events and behavior in foreign countries. "These measures are employed to influence the policies of other governments, underline confidence in the leaders and institutions of these states, disrupt the relations between various nations, and discredit and weaken major opponents" [8]. They were also used to generate abroad favourable

[1] This section of the current analysis draws from [1]. See, also, the articles on Russian propaganda [2] and [3].

[2] See the perceptive discussion of Russian information policy [7].

views towards the Soviet Union and its policies and support for specific policy initiatives.[3]

2. The Collapse of the USSR and the Failed Democratisation of Russia

The dissolution of the Soviet Union in 1991 and the emergence of fifteen new states in its place seemingly brought to an end to the imperial tradition of Russian domination over various peoples conquered and absorbed into the Russian/Soviet empire over the period of more than half a millennium. Yet, since the very creation of the new Russian state, political leaders in Moscow have been committed to returning Russia to the status of a great power, including, since Vladimir Putin assumed power more than two decades ago, the reestablishment of much of the imperial political order that seemingly collapsed in 1991, and to using propaganda and disinformation in the pursuit of this and other goals. To a substantial degree, Western policy after the collapse of the former USSR assumed that Russia's demise as a great power would be a permanent characteristic of the international system and, thus "active measures" against the West would cease. Throughout the 1990s and after the turn of the century, Russia's interests and concerns were largely ignored, as both the United States and Western community more broadly moved to fulfill their own political and security objectives in post-Communist Europe – objectives that included the incorporation of most of Central and East European post-Soviet space into Western security, political and economic institutions.

Initially, as the Russian state found itself in virtual political and economic freefall under President Boris Yeltsin, the objective of reestablishing Russia's great power status seemed to be little more than a rhetorical and an unrealistic and unrealisable dream. Even though Russia did employ its greatly reduced military capabilities in the attempt to play a role in those Soviet successor states challenged by internal conflict – conflict often facilitated, if not initiated, by clandestine Russian military interference [13] – the prospect of the Russian Federation's rejoining the ranks of major global actors seemed remote until the domestic rise to power of President Vladimir Putin at the end of the century. However, as the Russian economy and Russian self-confidence and assertiveness were buoyed by the rising price of oil and gas, the revitalisation of other sectors of the economy, and the reassertion of Moscow's control over growing segments of the vast territory of the Russian Federation itself, more sophisticated diplomatic and economic instruments, including what amounts to

[3] Ladislav Bittman, the defected former head of the Soviet disinformation unit, described in great detail how he had mixed fact with fiction to create make-believe events and policies [10, pp. 5–6, 11]. For a detailed discussion of the broad disinformation campaign associated with the likely role of the USSR in the assassination of President John F. Kennedy, see [12].

economic blackmail,[4] became a central component of Russia's re-assertion of influence within what Moscow views as its traditional, and legitimate, sphere of influence. However, as events in Georgia since 2014 have made clear, brute military power remains an important element in the Russian arsenal. In effect, the Russian political leadership's initial commitment to integration into the "community of civilised states," to use Yeltsin's phrase [15], and its willingness to follow the Western lead on major international political issues, were short-lived. Even before 1995, President Yeltsin and Foreign Minister Andrei Kozyrev,[5] the primary architect of this pro-Western emphasis in Russian policy, were forced to redefine Russian foreign and security policy in a much more realistic and nationalistic direction than they had done initially [17]. Yet, the issue that raised the most serious response in Moscow in this period remained the question of NATO's expansion eastward. Moscow orchestrated a multifaceted campaign that included pressure on the applicant countries and threats that the expansion would, in effect, initiate a new cold war in relations between Russia and the West. In fact, however, when NATO decided to invite the Czech Republic, Hungary, and Poland to join the alliance, Russia reluctantly accepted the decision without any of the retaliatory responses that had been threatened. With Kozyrev's replacement as foreign minister by Georgii Primakov in 1996, Russia proclaimed a formal Eurasian thrust in its policy, one that included active Russian involvement in and primacy over the so-called "near abroad" of former Soviet territory.[6]

After Putin was appointed acting prime minister, and later replaced Yeltsin as Interim President on the last day of 1999, his commitment to reestablishing Moscow's control over domestic politics and to rebuilding the foundations of Russia's great power status, the financial boon resulting from the explosion of oil and gas prices, as well as the shortsighted and counterproductive policies of Washington, strengthened and expanded the range of policy instruments available to Russia, including economic and political leverage, in its ongoing attempts to reestablish its dominant role across post-Soviet space – the creation of a "Greater Russia" – as an integral part of reasserting its role as a great power whose interests could no longer be ignored as they were throughout the 1990s.[7]

3. The Return of Imperial Russia

But it was clear in the approach that Washington and its allies took to Moscow's objections to Western policy that Russia was not viewed in the restructured European security environment as an

[4] As Nygren [14, pp. 232ff.] demonstrated, economic levers became the most reliable instruments for Russia in its campaign to reassert control over its neighbours – at least until the military operations in Georgia.

[5] For an exceptional discussion of the specifics of Russian politics and of relations with the new ex-Soviet states see [16].

[6] For an excellent discussion of this shift in Russian policy toward the countries of the CIS (Commonwealth of Independent States) and the increased use of economic and financial instruments of power, see the work of Bertil Nygren [14, 18, 19].

[7] For an important collection of perceptive articles that examine the domestic and foreign policy dimensions of Russia's reemergence as a great power see [20, 21].

equal player whose interests had to be given serious consideration. Once it became obvious that their efforts to forestall the expansion of NATO eastward were doomed to failure, the Russians seem to have accepted the reality and attempted to gain whatever benefits they could out of that acceptance. They shifted the focus of their opposition to NATO expansion from East-Central Europe to the Baltics. Moreover, on 27 May 1997, Moscow signed the Russia-NATO Founding Act that was supposed to provide clear parameters for the relationship between Russia and the Western Alliance. In return, Russia was granted membership in an expanded "G-8," although it was excluded from full participation in those "G-8" meetings at which meaningful decisions concerning international financial matters were likely to occur. Although Russia and the United States cooperated in a variety of security areas, these relationships did not fulfill Russian goals. Moreover, given the disastrous state of the Russian economy at the time, Moscow could have little hope of exercising any real influence within the group. At the same time, the Russia-NATO Founding Act also proved to be unsatisfactory as a model for Russia to pursue its foreign policy interests. Thus, by summer 2001, little more than half a year into the presidency of George W. Bush and one-and-a-half years into Vladimir Putin's presidency, the US-Russian relations were on an apparent collision course.[8] Russians were increasingly frustrated by Washington's obvious disregard to their role in world affairs and by the apparent the US lack of concern for Russian interests – as in the NATO bombing of Yugoslavia and in the US efforts to restrict Russian involvement in the development of oil and gas reserves in the Caspian Basin [23, 24]. Before we turn to a discussion of Russian policy in the Putin era – as a prelude to returning to the issue of disinformation as a tool in that policy, it is important to refer to the Chechen war because of its overall impact on many other aspects of Russian policy. Moreover, the ongoing Russian struggle to reassert control over Chechnya and to root out Chechen opposition to that effort brought Moscow into regular conflict with Georgia, whose government the Russians accused of harbouring and supporting Chechen separatists [24].

Therefore, the war in Chechnya was much more than simply an internal challenge to central authority within the Russian Federation; it also had a visible impact on relations with both near neighbours and the West. The Russian Federation's relations with the West, especially with the United States, were increasingly conflictual. Russia was no longer taken seriously as a major actor in world affairs, and its views and concerns – for example, NATO's campaign against Yugoslavia for its attempt to expel the majority of the ethnic Albanians from

[8] For a careful analysis of the state of Russian relations with the West at this time see [22].

Kosovo largely ignored Russia, based on the assumption that it was no longer an important or relevant actor.

Thus, when Vladimir Putin took over as interim president on 1 January 2000, he inherited these and an entire series of additional policy disagreements with the United States, and the West more generally, that included the restructuring of the Russian debt, NATO, and European Union (EU) expansion, the US commitment to move forward with a missile defense system, the longer-term future of Yugoslavia and the Balkans, Russia's nuclear relations with Iran, and so on. The general parameters of Russian policy, including policy towards the United States, were set early in Putin's presidency, and derived directly from the policy lines established in Moscow in the mid-1990s. Putin made clear his commitment to reestablishing the place of Russia as the preeminent regional power and as an important international actor. Essential preconditions for the fulfillment of these objectives, as the "Foreign Policy Concept" that Putin approved indicated, were the internal political stability and economic viability of Russia [25, 26].[9] According to this policy prescription, Russia had to overcome all efforts towards and evidence of separatism, national and religious extremism, and terrorism. Putin moved forcefully, and in most cases effectively, in reasserting central governmental control in Russia [27]. The economy, while still not flourishing, had shown strong signs of turning around with growth rates of 4.5%, 10.0%, and 5.0% in the years 1999–2001. In the foreign policy arena, Putin continued to seek allies who shared Russia's commitment to preventing the global dominance of the United States that represents, in the words of the Foreign Policy Concept (2000), a threat to international security and to Russia's goal of serving as a major centre of influence in a multipolar world. Putin's success in dealing with the major problems challenging the Russian state at the beginning of the decade meant that Russia now faced the United States and the West from a position of increased strength. Besides rebuilding the foundations of the Russian state at any cost as a precondition of Russia's ability to reassert itself as a major power, Putin and his associates did benefit greatly, but not exclusively, from the exponential rise in global demand for gas and oil and the ensuing revitalisation of the Russian economy. This, in turn, contributed to Russia's ability to pursue a much more active and assertive foreign policy, as many analysts have noted [28–30].

[9] For an assessment of Imperial and Russian expansionist policy see [27].

3.1. Military Intervention, Economic Coercion, and the Rebuilding of "Greater Russia"

Before turning to the role of "information warfare" and disinformation in Russia's attempt to re-establish its great power status, a discussion of the reintegration of former Soviet space, which some have termed *Greater Russia,* precisely the policy implied by Putin's negative reference to the dissolution of the USSR, is required. As already noted, despite the rhetorical commitment of Russian leaders to deal with the former Soviet republics as sovereign equals, from almost the very creation of the Russian Federation, Moscow has been directly and indirectly involved in the internal affairs of its new neighbours [27]. Throughout the 1990s, the major instruments used to re-establish Russia's influence were various types of *de facto* military intervention and efforts to turn the Commonwealth of Independent States (CIS) into a meaningful organ of economic and political reintegration. Since at least 2000 Russian policy towards its neighbours in the CIS, as well as to the Baltic states, has become much more sophisticated and complex, though by no means more cooperative and neighbourly, culminating in the unjustified invasion of Ukraine in 2022 – and has relied increasingly, besides military means, on the use of Russia's dominant position in the energy field and its growing economic leverage vis-à-vis its much weaker and economically dependent neighbours. Most important has been the Russian government's regaining almost total control over Russian energy production and distribution and its dominating the energy sector of neighbouring countries – often through the semi-coerced purchase of the energy distribution and processing infrastructure of those countries [14, pp. 238–245, 19, 31]. As noted above, the exponential increase in global demand for energy has been the single most important factor fueling the revival of the Russian economy and to growing Russian political influence vis-à-vis neighbouring states [9, 14, 18, 19].[10] In fact, almost from the very inception of the new Russian Federation, Moscow has used its control of energy as a means to "influence" other former Soviet republics to change political positions that they had taken or to follow Moscow's policy lead. This has been especially true in Russia's relations with the Baltic republics, with Ukraine, Georgia, and more recently even with Belarus, all post-Soviet states with which Russia has had serious policy differences over the course of the past 15 years. Moscow has in all cases put the blame for the cut-off of energy flows on the other side, or explained them as the result of technical problems, and argued, as well, that the policies of its oil and gas companies were dictated solely by economic, not political, considerations.[11]

[10] The dominant narrative in analyses of Russia's economic revival that attribute, almost exclusively, to Russian gas and oil exports and to the rise in global demand and, thus, prices for those exports have been increasingly challenged by those who point to the vibrant growth of other sectors of the Russian economy. A recent World Bank report notes, for example, that growth in the Russian economy has been stimulated by sectors other than simply gas and oil. The report noted: "In 2003–04, oil and some industrial sectors drove economic growth, but the subsequent expansion was driven largely by non-tradable goods and services for the domestic market, including manufacturing goods. In 2007, wholesale and retail trade alone accounted for almost a third of economic growth. Booming construction and manufacturing contributed another 30%. Manufacturing expanded by 7.4% in 2007, up from 2.9% in 2006. By contrast, growth in resource extraction virtually stopped, reflecting capacity constraints. The good news, so far, is that high rates of productivity growth underlie this robust growth" [32, p. 4].

[11] It is important to recognise that, with the collapse of the former Soviet Uniont he Russian Federation decided to continue to supply gas and oil to other former republics–now, new sovereign states – at pricessubstantially below the world market price. ...

All of these countries are energy poor and almost totally dependent on supplies of petroleum, natural gas, and, in some cases, electricity imported from the Russian Federation [31]. after the opening

Nygren [19] refers to as the "tap weapon" – by stopping the delivery of oil and/or gas to these countries – on various occasions as a means of strengthening its position in policy disputes and negotiating situations. The dispute with Ukraine in 2005–2006, which resulted in Russia's cutting off exports of gas in the middle of winter – resulted from Gazprom's decision to more than triple the price of gas. This decision, however, emerged only in the aftermath of the "Orange Revolution," which had reversed the "victory" of Russia's preferred candidate in the Ukrainian presidential election a decade earlier. Until that time, Putin's policy towards Ukraine had been based on pragmatic long-term political and economic considerations. However, with the collapse of pro-Russian political forces in Ukraine, Russia expanded a more coercive approach to demonstrate to the Ukrainians that assertions of independence from Moscow's influence would have real costs [33, pp. 80–89]. The "gas war" of 2005–2006 between Russia and Ukraine was "resolved" by a complicated settlement in which a majority Russian-owned Swiss company sold gas originating supposedly from Central Asia to Ukraine at subsidised prices, with prices increasing gradually over several years to world market levels.[12]

Ukraine is by no means the only post-Soviet state to have experienced Moscow's political displeasure and, thus, the effects of the "tap weapon." Belarus, which for most of the post-Soviet period has pursued a slavishly pro-Russian policy, angered Putin's government in 2002, thereby leading to 4 years of confrontation between the two countries, with Gazprom taking the lead role in the dispute. Once again, because pipelines to the West crossed Belarusian territory, Belarus had some bargaining power. Eventually, however, the government of President Alexander Lukashenko was forced to capitulate or face the cut-off of Russian gas supplies. Prices were to be increased over a five-year period, while Gazprom gained direct control over the pipelines across Belarus [14, pp. 76–79].

Until the August 2008 Russian invasion of Crimea, the gas weapon, as well as that of electricity, had been the most important instrument in Russian pressure brought against Georgia in order to coerce the latter into policies more in line with Moscow's interests. Here, these pressures have been employed, along with traditional threats of military intervention in support of Abkhaz and South Ossetian separatists – threats that were realised in August 2008 [34]. In the Georgian case over the past several years Russia acquired substantial

...Thus, as global prices for gas and oil skyrocketed after the turn of the century, Russia was exporting oil and gas to neighbouring countries at subsidised prices one-third or less of the world market price.

[12] Nygren [14, pp. 61–62] provides a detailed discussion of the specifics of the agreements, as well as the relevant sources. Ukraine was in a position to bargain with Gazprom and Moscow because Russia depended upon the secure flow of gas through pipelines across Ukraine in order to fulfill its export obligations to customers in Central and Western Europe. See also [30].

[13] In 2003 the Russian firm UES obtained 75 percent ownership in a Georgian electricity distribution company and management control over several power plants, as well as 50 percent ownership of a nuclear power plant. Gazprom acquired control of Georgia's main gas pipeline in 2005 in return for a restructuring of the latter's debt. In other words, Russia now directly controls much of Georgia's energy production and distribution and still serves as the primary source of gas, even after the opening of the new pipeline from Azerbaijan in late 2006 [37, 38].

ownership of energy production and distribution facilities in Georgia to cover the costs of outstanding debts and as a precondition for continued discounted prices on Russian gas [35, 36].[13] This control, however, did not restrain the Georgian government into accepting Russian dominance in the region – or accepting the de facto autonomy of the Russian-backed secessions in South Ossetia and Abkhazia, resulting in military hostilities in August 2008 that in effect wiped out Georgian military capabilities developed in recent years with the US military assistance and training.[14]

Russia's *de facto* control over the energy supplies of other post-Soviet states – Armenia, Moldova, and the Baltic states – has also been used in similar ways to influence the policy positions of these countries, as Nygren [14] has described in some detail. Yet, there is another part of Russia's use of its domination over energy production and distribution that is significant for the drive to re-establishing Greater Russia and re-establishing the Russian Federation as a major world power, namely, attempting to gain control over the distribution of oil and gas from Central Asia in Western markets.

3.2. Russian Foreign Policy and Disinformation

As we have already seen, with the turn of the millennium Russian relations with both many newly independent former Soviet republics and the states of the West deteriorated appreciably, some to the point of warfare. Military and economic tools were increasingly the means used by Moscow to gain its objectives. However, propaganda and disinformation, as had been the case with the USSR, also emerged as important instruments with which to achieve foreign policy goals. We, therefore, examine the Russian conception of disinformation and the institutional framework within which it is carried out as well as the most important targets and themes emphasised recently.

In post-Communist Russia various academic views of information warfare have emerged that, in fact, define the same activity: "The process of undermining a legitimate government by manipulating the information domain in order to influence political elites and instill political dissent, separatism, and social strife within a given system" [42].[15] This concept describes, in the view of the Russian analysts, a Western technique to subvert its adversaries. In the opinion of Aleksandr Dugin, for example, the West (mainly the United States) has been waging an offensive against Russia throughout the 20th and early 21st century. Two directly political actions have been justified because of these views entering the political realm: The passage

[14] In early August 2008–after weeks of mutual verbal attacks between Moscow and Tbilisi and apparently with encouragement from political elements in the United States–President Saakashvili of Georgia, reportedly responding to rocket attacks from locations inside the breakaway region of South Ossetia, sent forces into the region to reincorporate the breakaway republic. The Russians, who had apparently massed troops on the Russian-South Ossetian border in advance, almost immediately overwhelmed Georgian forces in the republic, as well as in a second breakaway region of Abkhazia, and advanced far into Georgia territory proper [39, 40]. Among the most salient analyses of the Russian intervention is that of George Friedman [41], who points to the importance in Russia's calculations of what Moscow perceived–not without reason–as a U.S. policy of containment in which Georgia and Ukraine were important elements.

[15] In what well may be the best introduction to the topic available, along with that of Ofar Fridman [42] discusses the conceptual narratives for understanding information warfare: 'subversion-war' developed by Evgeny Messner [43], 'net-centric war' [44] and 'information warfare' developed by Igor Panarin [45]. These concepts all mean basically the same thing and underlie these authors' views of information warfare/ disinformation. ...

of domestic laws to limit the possibility of Western influence in Russia itself, and also the development of what have become global disinformation and other techniques of information warfare.[16]

By the middle of the first decade of the 21st century, Russian relations with much of the "near abroad" and with the West had already deteriorated significantly and Russian disinformation began to rise significantly. The outbreak of conflict with Ukraine in 2014 resulted in what Van Herpen [50, p. 1] calls "the Kremlin's most massive propaganda offensive in the past seventy years."[17]

3.3. Russian Information Warfare

Although "information warfare," or "disinformation policy" never disappeared completely after the demise of the USSR, it began to expand appreciably after Putin came to power and relations with both much of the "near abroad" and the West began to deteriorate as described by President Vladimir Putin, "We must take into account the plans and directions of development of the armed forces of other countries. Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive" [57]. In his *Handbook of Russian Information Warfare*, Giles [58, pp. 4, 22] explains the following:

> *Information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort, or destroy information. The channels and methods available for doing this cover an equally broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, You Tube videos, or direct approaches to individual human targets. Recent Russian campaigning provides examples of all of the above and more… Russia seeks to influence foreign decision-making by supplying polluted information, exploiting the fact that Western elected representatives receive and are sensitive to the same information flows as their voters. When disinformation delivered in this manner is part of the framework for decisions, this constitutes success for Moscow, because a key element of reflexive control is in place.*
>
> *However, even if disinformation is not successfully inserted into the policy-making chain, and only spreads in mass and social media, the effect can be to create a permissive public opinion environment where Russian narratives are presented as factual. Moscow's potential gain at this level of influence is to win public support in adversary nations, and thereby attenuate resistance*

…For a broad discussion of the general aspects of information theory see [46]. For more on the issue, without sole regard to Russia, see [47].

[16] For an overview of the Putin government's gaining control over the internet at home, while also attempting to control it internationally, see [48]. For a broad survey of Russian policy views, see [49].

[17] For some excellent discussions of the breadth and importance of disinformation policy since Russia's invasion of Ukraine, see [51–56].

> *to actions planned by Russia, in order to increase their chances of success and reduce the likelihood of damaging adverse reactions by the international community.*[18]

The range of targets is broad. Subversion campaigns can aim, as noted by two Russian analysts, primarily the mass media and religious organisations, cultural institutions, non-governmental organisations, public movements financed from abroad, and scholars engaged in research on foreign grants. All these institutions and individuals may be involved in a distributed attack and strike damaging point blows at the country's social system with the purported aims of promoting democracy and respect for human rights [60].

Obvious targets for distributing disinformation are the media, and a direct link is seen between media campaigns and society's capacity to resist. Social media are also an important tool in Russia's campaign [61]. The Russian analysts, Chekinov and Bogdanov, note that the

> *mass media today can stir up chaos and confusion in government and military management of any country and instill ideas of violence, treachery, and immorality, and demoralize the public. Put through this treatment, the armed forces personnel and public of any country will not be ready for active defense* [62].

However, organisations other than the media can also be targeted.

3.4. Russian Information Warfare in the Post-Communist World[19]

We shall now briefly examine some of the examples of Russian "information warfare" in the post-Communist world and the responses of the target states to the attacks. Among the first major campaigns orchestrated by Moscow was that against Estonia in 2007, when the Estonians had the audacity to move a Soviet World War II statue from the centre of the capital to a military cemetery on the edge of the city, resulting in the Bronze Soldier conflict [65]. Given that about 26% of the population of the country – significantly more in urban areas – consists of ethnic Russians (slightly more including all Russian speakers), this was an issue that greatly divided society. The Estonian government responded to widespread Russian actions by pursuing a policy and establishing an agency committed to an active approach to integration of non-Estonian speakers into the broader society and a response to Russian "information warfare" policy [63, pp. 49 ff.]. Also, among the most active and invasive programmes in post-Communist Europe and much of the

[18] As already noted above, the treatment of Russian "information warfare" is exceptionally perceptive. For a more general discussion that places Russian policy in the context of disinformation more generally, see [59].

[19] One of the most comprehensive treatments of Russian information warfare against former Communist states is the examination of information wars against Estonia, Georgia, Poland, Ukraine, and the Czech Republic [63]. As noted in [63], the primary purpose of information warfare is to drive political wedges between competing population groups in target countries. This is very often accomplished by projecting information that is largely, or fully, true but is likely to contribute to political conflict in target countries. Moreover, Stengel [47] places Russian policy in the context of that of China and others. For another comprehensive study, see [64].

rest of the world has been its campaign for support of its policy in Crimea. Linked to quite tense relations between the two countries, sometimes Western opposition to Russian policy has been tied to the latter's engagement in a major disinformation and propaganda campaign to support its intervention and seizure of territories in Crimea [46],[20] but backed it up with continued military pressure, as well as propaganda, against Georgia [67]. Similarly, Russia mounted major disinformation campaigns targeted across Eastern Europe, especially against Ukraine [68].

The question arises, what one can do to respond to and counter Russian disinformation? "Western countermeasures have raised awareness of Russian activities, but their impact on Russia's efforts has been uncertain, and Russia appears undeterred" [61, 69, 70]. In the cases of Estonia and the Czech Republic, both countries recognised Russian information warfare and have been quite effective in countering it by establishing government agencies to detect and counter Russian efforts, and by engaging think tanks and citizen volunteers in countering it, among many other approaches [71], including an attempt by Estonia to get the EU to create an agency to deal with the issue. Elsewhere in Europe, Sweden has invested heavily in a comprehensive approach to combating foreign interference in their democracy, and their efforts have largely been successful. This begins to occur in other post-Communist states [72]; moreover France successfully prevented Russian interference in its elections and in Putin's attempts to divide the French society [70]. The Russian Internet Research Agency (IRA) had a role in the very close election held in the United Kingdom to leave the EU [73].

The most comprehensive answer to the question of how to respond, however, is given by Vilmer [74], who provides a list of policy recommendations that he views as useful – or necessary – to counter Russian disinformation, from distinguishing disinformation and propaganda from public diplomacy to defending European values[21]. Many of the suggestions on this list are derived from the experiences of European countries [75].

3.5. Russian Disinformation Policy in the Developing World

The Russians have also been very active to – generally successful – disinformation tactics in the developing world, possibly with special focus on Africa, but also on other regions. They have extended their global disinformation campaign to Africa, where they promote pro-Russian and anti-Western attitudes through

[20] For a discussion of various means to counter Russian "information warfare" see [66].

[21] The entire list of Vilmer's [74] recommendations includes the following:

1. Distinguish disinformation and propaganda from public diplomacy
2. Do not engage in Russophobia or demonising Putin
3. Note publicly that the issue is important
4. Recognise that there is a continuum between military actions and information warfare
5. Understand the subject well by re-enforcing research on the subject
6. Recognise the limits of a solely governmental response and the need for a global one
7. Recognise the limits of refutation and that pointing out the truth is insufficient
8. Create the largest and youngest and the most educated audience possible that thinks critically
9. Promote a journalistic ethics charter signed off by the media of all countries
10. Adapt response to the listener
11. Encourage the development of independent Russian media that is not state-financed
12. Translate and promote the work of independent Russian journalists
13. Invite the most promising of independent to join a programme
14. Point out the old witnesses of Russian disinformation that expose the methods used
15. Use the technology available for fact-checking and to identify trolls, including Facebook and Twitter

propaganda and disinformation. After each disinformation campaign, Moscow assesses its efforts and then tweaks tactics, accordingly, adapting to new countermeasures as necessary. This campaign is centred in and focused on numerous African countries and has been a blending of Kremlin propaganda and local content. Disinformation campaigns in Africa have been elevated to a centerpiece of Russia's foreign and security policy [76].

As Grossman [77] demonstrates, the Russians have been employing social media in Africa to support local regimes and to oppose Western interests and policies. Russia is also running some of its campaigns against the United States and Western Europe out of Africa [78]. Comparable campaigns have been carried out in Latin America, where Twitter and other social media accounts have been very active in supporting accounts that Russia has been "playing a geopolitical role in this hemisphere against what they consider its main enemy – the United States," noted Carlos Vecchio, the Venezuelan envoy in Washington [79].[22] The overall importance of the media – and of the ability to project the Russian "story" – can be seen in the fact that Russia has announced the commitment of a million dollars for the expansion of "independent" media in developing countries [80].

3.6. Russian Disinformation Policy in the West

As pointed out early in this article, although Russian disinformation policy has expanded dramatically across the world in recent years, the one focused on the West – on Europe and the United States – has remained by far the most extensive campaign. Cosentino [81] and many others have shown in some detail that even the US and other elections have not been beyond the reach of the Russian Internet Agency (IRA),[23] although the overall impact of their involvement is not clear. The Russians have attempted, both during and outside election cycles, to support candidates whom they favour and to contribute to the political divisions that exist in Western societies [71, 86].

These Russian attacks involve transparently false stories, as well as partially true ones that are meant to cause dissension and political chaos in the target states.[24] Across Western Europe, the Russians have established radio stations and other communications facilities in Germany, Switzerland, and elsewhere that broadcast to West European audiences and thereby, as the Russians hope, have an impact on them [91]. Moreover, there is clear evidence in the United States that many of the vitriolic exchanges supposedly between domestic political factions in reality stem from Russian sources – via

16. Re-enforce the European task force by providing sufficient funds and personnel
17. Encourage European states to develop national means for the fight against disinformation
18. Re-enforce cooperation among states, the EU, and NATO in this area
19. For each false information not only correct the content but also expose the method used
20. Point out the source of financing
21. Create an international organisation dedicated to fighting disinformation
22. Consider more restrictive countermeasures, such as fines and sanctions
23. Counter not only disinformation but also its intent and potential effects by strengthening what it seeks to weaken
24. Communicate more effectively in Russian, especially on social networks
25. Assume and defend European values and develop a positive discourse.

For another list of actions to thwart Russian policy, see [70].

[22] For a general discussion of Russian policy in Latin America, including disinformation policy, see [84].

[23] See [82] concerning the role of the Internet Research Agency (IRA) in carrying out Russian disinformation policy; see also [48, 83–85].

[24] See [73, 89] for the different aspects of Russian disinformation activities in the EU; in German, see [90].

Facebook, for example, by which an estimated 140 million Americans a month were reached via Russian trolls prior to the US election in 2020 [82, 92].

Among the more important issues addressed in this Russian campaign to undermine, or at least cause disruption, even chaos, in Western political systems have been those associated with the global COVID 19 pandemic [93]. Russian disinformation sources have questioned the efficacy of the vaccines developed to deal with the disease and, thus, have contributed to the concern about them and the refusal to take them in the West – especially in the United States [94, 95].

A study of disinformation in the United States concluded that the most affected audience has been a politically conservative one [96].[25] The result is an undercutting of mainstream views and the emergence of opposition to government policy on masks, vaccines, political issues, and related matters. The finding that there is more impact of Russian policy on the political right is borne out by the position taken on numerous international political issues by conservative commentators such as Tucker Carlson [99], formerly of Fox News and Senators like Ted Cruz of Texas [100], who basically opposed President Biden and supported Putin of Russia on his threat to invade Ukraine, a US ally. For Tucker Carlson [99], Cruz [100], and others, such as Representative Marjorie Taylor Green on the far right, the United States has pursued policies in Central and Eastern Europe since the demise of the USSR that have challenged Russia's regional interests and, thus, Putin can be expected to and is justified in challenging Ukraine and indirectly the United States, as it is currently doing. Thus, the US support for Ukraine should be downplayed, even eliminated.

4. Towards the Future

What is now clear across most of the globe is the fact that Moscow is involved on a massive scale in the attempt to manipulate the views of the populations and elites of other countries on all sorts of political issues – from the local ones to issues of Russian – Western confrontation. In some cases, the objective is to justify Russian intervention, as in Georgia and Ukraine. In others, it is to support local political elites that favour Russian positions on global or regional issues.[26] In yet other cases, it is to drive a wedge between developing countries and the West. Additionally, as in the disinformation campaign on the ineffectiveness of the Western anti-COVID 19 vaccines, it is meant to contribute to political chaos in other countries to weaken opposing governments.

[25] In 2022 a growing portion of the right wing of the Republican party de facto supported Russia in its war against Ukraine [97].

[26] This position is widely held among those of the political center and left for the U.S. presidential elections of 2016 and 2020 and borne out by much official intelligence [95, 101].

As proposed by the Russian academic theorists of information warfare, Moscow must use all means possible to weaken and to contain the impact of disinformation of its opponents and project its own while systematically denying engagement in such activity [42]. One advantage that other states now have learned, compared to a decade ago, the fact that Russian disinformation policy is well known and some states – especially in East-Central Europe and Scandinavia – have developed effective means to limit the impact of Russian information warfare. Other states, therefore, can learn from them. Yet the costs, in terms of alertness and in devoting substantial effort to containing the impact of propaganda and disinformation, remain very significant.

Acknowledgements

This paper is published posthumously. Special thanks go to Professor Kanet's grandson, Christopher K. Zelle, without whose dedicated assistance the writing of this paper would not have been possible. The ACIG editorial team would like to express our deep gratitude to the family of Professor Roger E. Kanet for their support and approval of the final version of this manuscript for publication. Their consent has been invaluable in honoring Professor Kanet’s legacy and contributions to the field.

References

[1] R.E. Kanet, “Soviet propaganda and the process of national liberation,” in *Contemporary Soviet Propaganda and Disinformation. A conference report,* A. Salter, Ed. (assisted by W.J. Colligan), Washington DC: U.S. Department of State, Publication No. 9536, 1987, pp. 215–254. [Online]. Available: https://www.google.com/search?client=firefox-b-1-d&q=Soviet+Propaganda+and+the+Process+of+National+Liberation. [Accessed: Oct. 15, 2023].

[2] C. Paul, M. Matthews, *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND, 2016. [Online]. Available: https://www.rand.org/pubs/perspectives/PE198.html. [Accessed: Oct. 15, 2023].

[3] R.E. Kanet, “Soviet Propaganda and the process of national liberation,” *ACDIS Occasional Paper*, 1985.

[4] Pechat’ v USSR. Moscow: Finansy i Statistiski, 1983.

[5] S.P. Sanakoev, *Voprosy sovetskoi vneshnepoliticheskoi propagandy*. Moscow: Mezhdunarodnye Otnoshenia, 1980.

[6] B.A. Hazan, *Soviet Propaganda: A Case Study of the Middle East Conflict.* Jerusalem: Israel Universities Press, 1976.

[7] G. Wilde, J. Sherman, *No Water's Edge: Russia's Information War and Regime Security*. Washington, DC: Carnegie Endowment for International Peace, 2023. [Online]. Available: https://carnegieendowment.org/2023/01/04/no-water-s-edge-russias-information-war-and-regime-security-pub-88644?utm_source=carnegieemail&utm_medium=email&utm_campaign=announcement&mkt_tok=g. [Accessed: Oct. 15, 2023].

[8] R.H. Shultz, R. Godson. *Dezinformatsia: Active Measures in Soviet Strategy.* New York, NY: Pergamon-Brassey's, International Defense Publishers, 1984.

[9] E. Pond, "Disinformation. A four-part series," *The Christian Science Monitor,* Feb. 26, pp. 16–17; Feb. 27, pp. 16–17; Feb. 28, pp. 14-15, and Mar. 1, pp. 16–17.

[10] T. Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. New York, NY: Farrar, Straus and Giroux, 2020.

[11] L. Bittman, "Interview with Thomas Rid," 25 Mar. 2017, Rockport, MA. Audio. [Online]. Available: https://archive.org/details/bittman-ridt. [Accessed: Oct. 15, 2023].

[12] R.J. Woolsey, I.M. Pacepa, *Operation dragon: The Kremlin's secret war on America.* New York: Encounter, 2021.

[13] A.V. Kozhemiakin, R.E. Kanet, "Russia as a regional peacekeeper," in *Resolving Regional Conflicts*, R.E. Kanet, Ed. Champaign, IL: University of Illinois Press, 1998, pp. 225–239.

[14] B. Nygren, *The rebuilding of Great Russia. Putin's foreign policy towards the CIS countries*. London and New York: Routledge, 2008.

[15] B. Yeltsin, "Boris Yeltsin on Russian Television," 14 February; cited in S. Crow, "Russian Federation faces foreign policy dilemmas," *RFE/RL Research Report,* vol. 1, no. 10, 1992, pp. 15-19.

[16] A. Kozyrev, *Fire Bird: The Elusive Fate of Russian Democracy.* Pittsburgh: University of Pittsburgh Press, 2019.

[17] A.P. Tsygankov, P.A. Tsygankov, "Constructing National Values: The Nationally Distinctive Turn in Russian IR Theory and Foreign Policy," *Foreign Policy Analysis*, vol. 17, no. 4, 2021, doi: 10.1093/fpa/orab022.

[18] B. Nygren, “Putin’s Attempts to Subjugate Georgia: From Sabre-Rattling to the Power of the Purse,” in *Russia: Re-Emerging Great Power*, R.E. Kanet, Ed. Houndmills, UK: Palgrave Macmillan, 2007, pp. 107–123, doi: 10.1057/9780230590489_6.

[19] B. Nygren, “Putin’s Use of Natural Gas to Reintegrate the CIS Region,” *Problems of Post-Communism*, vol. 55, no. 4, pp. 3–15, 2008, doi: 10.2753/PPC1075-8216550401.

[20] J. Hedenskog, V. Konnander, B. Nygren, I. Oldberg, C. Pursiainen, *Russia as a Great Power. Dimensions of security under Putin*. London and New York: Routledge, 2005.

[21] V. Rukavishnikov, “Choices for Russia: Preserving inherited geopolitics through emergent global and European realities,” in *Russia: Re-Emerging Great Power*, R.E. Kanet, Ed. Houndmills, UK: Palgrave Macmillan, 2007, pp. 54–78, doi: 10.1057/9780230590489_4.

[22] A. Kassianova, “Russia: Still open to the west? Evolution of the state identity in the foreign policy and security discourse,” *Europe-Asia Studies,* vol. 53, no. 6, pp. 821–839, 2001, doi: 10.1080/09668130120078513.

[23] R. Ebel, R. Menon*,* Eds., *Energy and Conflict in Central Asia and the Caucasus*. Lanham, MD: Rowman & Littlefield, for the National Bureau of Asian Research, 2000.

[24] R.E. Kanet, L. Homarac, “The U.S. challenge to Russian influence in Central Asia and the Caucasus,” in R*ussia: Re-emerging Great Power,* R.E. Kanet, Ed. Houndmills, UK: Palgrave-Macmillan, 2007, pp. 173–194, doi: 10.1057/9780230590489_9.

[25] Foreign Policy Concept. (Jun. 28, 2000). The foreign policy concept of the Russian Federation, approved by the President of the Russian Federation V. Putin. [Online]. Available: *Johnson’s Russia List,* no. 4403. http://www.cdi.org/russia/johnson/. [Accessed: Oct. 15, 2023].

[26] Kontseptsiia natsional’noi bezopasnosti. Kontseptsiia natsional’noi bezopasnosti Rossiiskoi Federation. (Jul. 11, 2000). *Nezavisimoe voennoe obozrenie* (Internet version). [Online]. Available: http://nvo.ng.ru/concepts/2000-0114/6_concept.html. [Accessed: Oct. 15, 2023].

[27] R.E. Kanet, “Rebuilding a ‘greater Russia’ and the Russian invasion of Ukraine,” *Transatlantic Policy Quarterly*, vol. 22, no. 1, 2023. [Online]. Available: http://transatlanticpolicy.com/article/1195/rebuilding-greater-russia-and-the-invasion-of-ukraine. [Accessed: Oct. 15, 2023].

[28] K.J. Hancock, “Russia: Great power image versus economic reality,” *Asian Perspective,* vol. 31, no. 4, pp. 71–98, 2007, doi: 10.1353/apr.2007.0003.

[29] M. McFaul, K. Stoner-Weiss, “The myth of Putin’s success,” *Foreign Affairs*, vol. 87, no. 1, pp. 68–84, 2008.

[30] A.J. Motyl, R. Menon, “The myth of Russian resurgence,” *The American Interest,* vol. 2, no. 4, pp. 96–101, 2007. [Online]. Available: https://www.the-american-interest.com/2007/03/01/the-myth-of-russian-resurgence/. [Accessed: Oct. 15, 2023].

[31] A. Gasparyan, “The role of energy in Russian foreign policy,” in *Russia and the World in the Putin Era: From Theory to Reality in Russian Global Strategy*, R.E. Kanet, Ed. London: Routledge, 2021.

[32] World Bank, *Russian Economic Report, No. 16*. Washington, DC: World Bank, 2008. [Online]. Available: http://siteresources.worldbank.org/INTRUSSIANFEDERATION/Resources/rer16_Eng.pdf. [Accessed: Oct. 15, 2023].

[33] J. Bugajski, *Cold Peace: Russia’s New Imperialism.* Westport, CT: Praeger, 2004.

[34] The Economist (May 15, 2008). “Georgia and Russia: Gather round the Gorge.” [Online]. Available: https://economist.com/leaders/2008/05/15/gather-round-the-gorge. [Accessed: Oct. 15, 2023].

[35] R. Giragosian, “Shifting security in the South Caucasus,” *Connections: The Quarterly Journal,* vol. 6, no. 3, pp. 100-106, 2007. [Online]. Available: https://connections-qj.org/article/shifting-security-south-caucasus. [Accessed: Oct. 15, 2023].

[36] A.N. Pamir, “Energy and pipeline security in the Black Sea and Caspian Sea regions: Challenges and solutions,” in *The Black Sea Region: Cooperation and Security Building,* O. Pavliuk, I. Klympush-Tsintsadze, Eds. Armonk, NY: M.E. Sharpe, 2003, pp. 123–155.

[37] H. Khachatrian, “Russian moves in Caucasus energy and power sectors could have geopolitical impact,” *Eurasia Insight,* 2003.

[38] I. Torbakov, “Emulating Global Big Brother: The Ideology of American Empire and Its Influence on Russia’s Framing of Its Policies in the Post-Soviet Eurasia,” *Turkish Review of Eurasian Studies*, vol. 3, pp. 41–72, 2003.

[39] R. Giragosian, “Georgian planning flaws led to campaign failure,” *Jane’s Defence Weekly,* vol. 15, 2008.

[40] J.L. Galloway, “A bad neighbor in a bad neighborhood,” *The Miami Herald,* 17 Aug. 2008.

[41] G. Friedman, "Georgia and the balance of power," *The New York Review*, 25 Sep 2008. [Online]. Available: https://www.nybooks.com/articles/2008/09/25/georgia-and-the-balance-of-power/. [Accessed: Oct. 15, 2023].

[42] O. Fridman, The Russian perspective on information warfare: Conceptual roots and politicization in Russian academic, political, and public discourse. *Defence Strategic Communications*, vol. 2, no. 2, 2017, pp. 61–86, doi: 10.30966/2018.riga.2.3.

[43] O. Fridman, *Russian "hybrid warfare": Resurgence and politicization*. Oxford: Oxford University Press, 2018, doi: 10.1093/oso/9780190877378.001.0001.

[44] A. Dugin, "The belt and road initiative: A Eurasian road," Russian strategist Dr. Alexander Dugin interview by Fikret Akfirat. *Belt & Road Initiative Quarterly, vol. 1, no.* 4, pp. 6–18, 2020. [Online]. Available: https://briqjournal.com/en/russian-strategist-dr-alexander-dugin-the-belt-and-road-initiative-eurasian-road. [Accessed: Oct. 15, 2023].

[45] G. Bolding, "The Panarin nightmare: A hypothetical dissolution of the United States revisited," *An Injustice!* 29 Dec. 2020. [Online]. Available: https://aninjusticemag.com/the-panarin-nightmare-442cf75692e8. [Accessed: Oct. 15, 2023].

[46] J. Darczewska*, The Anatomy of Russian Information Warfare. The Crimean Operation, A Case Study*. Warsaw: The Centre for Eastern Studies, 2014.

[47] R. Stengel, *Information Wars: How We lost the Global Battle against Disinformation & What We Can Do About It*. New York, NY: Grove Press, 2019.

[48] A. Soldatov, I. Borogan. *The Red Web: The Kremlin's War on the Internet.* New York, NY: Public Affairs, 2015.

[49] US Department of State. *Pillars of Russia's disinformation and propaganda ecosystem. GEO special report.* Washington, DC: GEO, 2020. [Online]. Available: https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/. [Accessed: Oct. 15, 2023].

[50] M.H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Policy.* New York, NY: Rowman & Littlefield, 2015.

[51] S. Bushwick, "Russia's information war is being waged on social media platforms, but tech companies and governments are fighting back," *Scientific American*, 8 Mar. 2022. [Online]. Available: https://www.scientificamerican.com/article/russia-is-having-less-success-at-spreading-social-media-disinformation/. [Accessed: Oct. 15, 2023].

[52] Global Engagement Center, *Disarming disinformation: Our shared responsibility*. Online, 2022. Update 31 Aug. 2022. [Online]. Available: https://www.state.gov/disarming-disinformation/. [Accessed: Oct. 15, 2023].

[53] A. Legucka, "Russia's long-term campaign of disinformation in Europe," Carnegie Europe, 19 Mar. 2020. [Online]. Available: https://carnegieeurope.eu/strategiceurope/81322. [Accessed: Oct. 15, 2023].

[54] NPR. *Russian businessman linked to Putin admits to U.S. election meddling*. NPR, 7 Nov. 2022. [Online]. Available: https://www.npr.org/2022/11/07/1134878028/yevgeny-prigozhin-russia-election-interference-putin. [Accessed: Oct. 15, 2023].

[55] C. Smith, B. Cardin, Ben. The scourge of Russian disinformation. Commission on Security and Cooperation in Europe, 14 Sep. 2017. [Online]. Available: https://www.csce.gov/international-impact/events/scourge-russian-disinformation. [Accessed: Oct. 15, 2023].

[56] The Associated Press, "Twitter aims to crack down on misinformation, including misleading posts about Ukraine," 19 May 2022. [Online]. Available: https://www.npr.org/2022/05/19/1100100329/twitter-misinformation-policy-ukraine. [Accessed: Oct. 15, 2023].

[57] V. Putin. (May 11, 2006). "Soldier' is an honourable and respected rank. Excerpts from annual Address to the Federal Assembly of the Russian Federation," *Krasnaya Zvezda*. [Online]. Available: http://old.redstar.ru/2006/05/11_05/1_01.html. [Accessed: Oct. 15, 2023].

[58] K. Giles, *Handbook of Russian Information Warfare.* Rome: NATO Defense College, 2016.

[59] P. Pomerantsev, This Is Not Propaganda: Adventures in the War against Reality. New York, NY: Public Affairs, 2018.

[60] S.G. Chekinov, S.A. Bogdanov, "The nature and content of a new-generation war," *Military Thought* (English edition), no. 4, pp. 12–23, 2013.

[61] E. Treyger, J. Cheravitch, R.S. Cohen, *Russian Disinformation Efforts on Social Media.* Santa Monica, CA: RAND, 2022. [Online]. Available: https://www.rand.org/pubs/research_reports/RR4373z2.html. [Accessed: Oct. 15, 2023].

[62] S.G. Chekinov, S.A. Bogdanov, "Initial periods of wars and their impact on a country's preparations for a future war," *Military Thought* (English edition), vol. 21, no. 4, pp. 14–28, 2012.

[63] N. Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict.* London: I.B.Tauris, 2020.

[64] US Government Office. (Mar. 30, 2017). *Disinformation: A primer in Russian active measures and influence campaigns. Hearing before the Select Committee on Intelligence.* Washington, DC: US Government Office. [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-115shrg25998/html/CHRG-115shrg25998.htm. [Accessed: Oct. 15, 2023].

[65] J. Heering, H. Kamboj, *Case 355 – Estonia: The First Battle in the Modern Disinformation War – Lessons for Democracies Fighting Hybrid Warfare*. Washington, DC: Institute for the Study of Diplomacy at Georgetown University, 2021.

[66] P. Pomerantsev, *This Is Not Propaganda: Adventures in the War against Reality*. New York, NY: Public Affairs, 2018.

[67] G. Shaishmelashvili, "Russia's permanent war against Georgia," Foreign Policy Research Institute*,* 2021. [Online]. Available: https://www.fpri.org/article/2021/03/russia-permanent-war-georgia/. [Accessed: Oct. 15, 2023].

[68] T.C. Helmus, E. Bodine-Baron, A. Radin, M. Magnuson, J. Mendelsohn, W. Marcellino, A. Bega, Z. Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Brussels: Council of the European Union, 2018.

[69] E. Bodine-Baron, T.C. Helmus, A. Radin, E. Treyger, *Countering Russian Social Media Influence*. Santa Monica, CA: RAND, 2018. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2740.html. [Accessed: Oct. 15, 2023].

[70] H. Conley, J.-B. J. Vilmer. *Successfully countering Russian electoral interference*. CSIS Briefs, 2018. [Online]. Available: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference. [Accessed: Oct. 15, 2023].

[71] CSIS. *Countering Russian Disinformation*. Center for Strategic & International Studies*,* 2020. [Online]. Available: https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation. [Accessed: Oct. 15, 2023].

[72] A. Ellick, A. Westbrook. "Operation Infektion: How Russia perfected the art of war," *NYT Opinion* (video), 2019. [Online]. Available: https://www.youtube.com/watch?v=tR_6dibpDfo&t=92s. [Accessed: Oct. 15, 2023].

[73] M.L. Taylor, "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe," *Brookings*, 2019. [Online]. Available: https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/. [Accessed: Oct. 15, 2023].

[74] J.-B.J. Vilmer, La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande? *Revue Défense Nationale*, no. 801, pp. 93–105, 2017. [Online]. Available: https://www.cairn.info/revue-defense-nationale-2017-6-page-93.htm. [Accessed: Oct. 15, 2023].

[75] T. Kent, *Striking Back: Overt and Covert Options to Combat Russian Disinformation.* Washington: The Jamestown Foundation, 2020.

[76] IntelBrief. (Nov. 7, 2019). *Russian disinformation in an African context*. [Online]. Available: https://thesoufancenter.org/intelbrief-russian-disinformation-in-an-african-context/. [Accessed: Oct. 15, 2023].

[77] S. Grossman, "Russian disinformation campaigns target Africa: An Interview with Dr. Shelby Grossman," Africa Center for Strategic Studies, 2020. [Online]. Available: https://africacenter.org/spotlight/russian-disinformation-campaigns-target-africa-interview-shelby-grossman/. [Accessed: Oct. 15, 2023].

[78] T. Hatmaker, "Russian trolls are outsourcing to Africa to stoke US racial tensions," TC, 12 March 2020. [Online]. Available: https://techcrunch.com/2020/03/12/twitter-facebook-disinformation-africa-ghana-nigeria-ira-russia/. [Accessed: Oct. 15, 2023].

[79] L. Jakes, "As protests in South America surged, so did Russian trolls on Twitter, US finds," The New York Times, 19 Jan. 2020. [Online]. Available: https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html. [Accessed: Oct. 15, 2023].

[80] The Moscow Times. (Aug. 2, 2021). *Russia to Invest $1 M in independent media in developing countries.* [Online]. Available: https://www.themoscowtimes.com/2021/08/02/russia-to-invest-1m-in-independent-media-in-developing-countries-a74668. [Accessed: Oct. 15, 2023].

[81] G. Cosentino, "Polarize and conquer: Russian influence operations in the United States," in *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation*. Cham: Palgrave-Macmillan, 2020, pp. 33–57, doi: 10.1007/978-3-030-43005-4_2.

[82] K. Hao, "Troll farms reached 140 million Americans a month on Facebook before 2020 election, internal report shows," *MIT Technology Review*, 2021.

[83] M. Hellman, C. Wagnsson, "How can European states respond to Russian information warfare? An analytical framework," *European Security*, vol. 26, no. 2, pp. 153–170, 2017, doi: 10.1080/09662839.2017.1294162.

[84] R.E. Kanet, D. Moulioukova, "Russia in Latin America: An extension of Moscow's policy in the developing world," *Global Affairs,* vol. 7, no. 3, pp. 295–310, 2021, doi: 10.1080/23340460.2021.1985940.

[85] P. Reltien, et Cellule investigation de Radio France. La menace d'une ingérence russe plane-t-elle sur les élections européennes? France Culture, 23 Mar. 2019. [Online]. Available: https://www.franceculture.fr/geopolitique/la-menace-dune-ingerence-russe-plane-t-elle-sur-les-elections-europeennes. [Accessed: Oct. 15, 2023].

[86] P. Reltien, Cellule investigation de Radio France, "La menace d'une ingérence russe plane-t-elle sur les élections européennes?" *France Culture,* 23 Mar 2019. [Online]. Available: https://www.franceculture.fr/geopolitique/la-menace-dune-ingerence-russe-plane-t-elle-sur-les-elections-europeennes. [Accessed: Oct. 15, 2023].

[87] A. Chen, "The agency. An investigation into the Russian troll farm called the Internet Research Agency," *The New York Times Magazine.* 7 Jun 2015*.* [Online]. Available: https://www.nytimes.com/2015/06/07/magazine/the-agency.html. [Accessed: Oct. 15, 2023].

[88] A. Weisburd, C. Watts, J.M. Berger, "Trolling for Trump: How Russia is trying to destroy our democracy," *War on the Rocks,* 16 Nov. 2016. [Online]. Available: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/. [Accessed: Oct. 15, 2023].

[89] L. Makhashvili, "The Russian information war and propaganda narratives in the European Union and the EU's Eastern partnership countries," *International Journal of Social Science and Humanity*, vol. 7, no. 5, pp. 309–313, 2017, doi: 10.18178/ijssh.2017.V7.840.

[90] M. Becker, "Darum ist Deutschland das Topziel für russische fake news," *Spiegel Politik*, 8 Mar. 2021. [Online]. Available: https://www.spiegel.de/politik/deutschland/darum-ist-deutschland-das-top-ziel-fuer-russische-fake-news-a-fab21190-979d-496a-93b4-c0b7d7446bca. [Accessed: Oct. 15, 2023].

[91] C. Reichmuth, "RT greift unsere Demokratie an: Russia today sendet bald aus Deutschland – und will auch in die Schweiz," *Luzerner Zeitung,* 2 Sep. 2021. [Online]. Available: https://www.luzernerzeitung.ch/international/putins-staatssender-rt-greift-unsere-demokratie-an-russia-today-sendet-bald-aus-deutschland-und-will-in-die-schweiz-ld.2182004?reduced=true. [Accessed: Oct. 15, 2023].

[92] A. Lardieri, "Russia still largest driver of disinformation on social media, Facebook report finds," U.S. News, 26 May 2021. [Online]. Available: https://www.usnews.com/news/politics/articles/2021-05-26/russia-still-largest-driver-of-disinformation-on-social-media-facebook-report-finds. [Accessed: Oct. 15, 2023].

[93] M.R. Gordon, D. Volz, "Russian disinformation campaign aims to undermine confidence in Pfizer, other Covid-19 vaccines, U.S. officials say," *The Wall Street Journal*, 7 Mar. 2021. [Online]. Available: https://www.wsj.com/articles/

russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200. [Accessed: Oct. 15, 2023].

[94] J. Vanian, "Russian disinformation campaigns are trying to sow distrust of COVID vaccines, study finds," *Fortune*, 23 July 2021. [Online]. Available: https://fortune.com/2021/07/23/russian-disinformation-campaigns-are-trying-to-sow-distrust-of-covid-vaccines-study-finds/. [Accessed: Oct. 15, 2023].

[95] J.E. Barnes, "Russian disinformation targets vaccines and the Biden Administration," *The New York Times,* 5 Aug. 2021; updated 18 Oct. 2021. [Online]. Available: https://www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html. [Accessed: Oct. 15, 2023].

[96] F. Hjorth, R. Adler-Nissen, "Ideological asymmetry in the reach of pro-Russian digital disinformation to United States audiences," *Journal of Communication*, vol. 69, no. 2, pp. 168–192, 2019, doi: 10.1093/joc/jqz006.

[97] J. Shapera, "Marjorie Taylor Greene: 'Under Republicans, not another penny will go to Ukraine," *The Hill*, 14 Nov. 2022. [Online]. Available: https://thehill.com/homenews/house/3719467-marjorie-taylor-greene-under-republicans-not-another-penny-will-go-to-ukraine/. [Accessed: Oct. 15, 2023].

[98] O. Olafimihan, "More Republicans opposed to continued Ukraine aid: Survey," *The Hill*, 3 Nov. 2022. [Online]. Available: https://thehill.com/homenews/3717304-more-republicans-opposed-to-continued-ukraine-aid-survey/. [Accessed: Oct. 15, 2023].

[99] P. Suciu, "Tucker Carlson accused of promoting Russian propaganda as Putin masses forces on Ukraine border," Forbes, 8 Dec. 2021. [Online]. Available: https://www.forbes.com/sites/petersuciu/2021/12/08/tucker-carlson-accused-of-promoting-russian-propaganda-as-putin-builds-up-forces-on-ukraine-border/. [Accessed: Oct. 15, 2023].

[100] T. Cruz, "Russian troops amassed on the border of Ukraine are President Biden's fault for surrendering to Putin and gifting him Nord Stream 2. Sen. Cruz on the Senate Floor Newsroom," Press release. 7 Dec. 2021. [Online]. Available: https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-on-the-senate-floor-russian-troops-amassed-on-the-border-of-ukraine-are-president-bidens-fault-for-surrendering-to-putin-and-gifting-him-nord-stream-2. [Accessed: Oct. 15, 2023].

[101] Intelligence Community. *Foreign threats to the 2020 US Federal elections*. Intelligence Community Assessment, 10 Mar. 2021. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf. [Accessed: Oct. 15, 2023].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Collaborating Pariahs: Does the Ukraine War Cement an Adversarial Cyber-Information Bloc?

Chris Bronk | Hobby School of Public Affairs, University of Houston, USA |
ORCID: 0009-0002-6778-2206

Received: 20.01.2024

Accepted: 23.05.2024

Published: 28.06.2024

Cite this article as:
C. Bronk, "Collaborating pariahs: Does the Ukraine war cement an adversarial cyber-information bloc?," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190263

Corresponding author:
Chris Bronk, Hobby School of Public Affairs, University of Houston, Houston, TX, USA. E-mail: rcbronk@Central.UH.EDU;
0009-0002-6778-2206

Abstract

Russia's 2022 invasion of Ukraine has dramatically altered global politics, not least that several so-called pariah states appear to be cooperating at a deeper level than at any time since the end of the Cold War. Occupying a critical position between the pariahs and the rest of the community of nations is China, an adversary to the United States, but not a pariah to the degree of Russia or its allies North Korea and Iran. Each of these countries has advanced both cyber and information operations. Considered here is a framework for understanding linkages between China and the pariahs; a chronicle of cyberattacks by each of the countries mentioned as well as consideration of possible collaboration; and observations on their propagandistic information operations since the beginning of the Russo-Ukraine War.

Keywords

cybersecurity, information influence, role theory

> *Russia is a country, but Russia plus Ukraine is an empire.*
> – Zbigniew Brzezinski

1. An Axis of Adversaries

When George Bush coined the term *axis of evil* in his 2002 State of the Union address, we could hardly imagine the current bloc of authoritarian nation-states cooperating to subvert the international order in place since the end of the Cold War. Where it was difficult to see Iran, Iraq, and the Democratic People's Republic of Korea (DPRK or North Korea) as able to dramatically influence global events through cooperative action, two decades later China and Russia have cultivated international partners whose influence may be found from the Korean Peninsula to the Esequibo area of South America [1]. This has profound meaning for cyber conflict, online influence campaigns, and the development of sophisticated military technology. With its invasion of Ukraine on 24 February 2022, Russia joined Iran and North Korea in the world's club of pariah states [2].

Russia's general invasion of Ukraine in 2022 also represents *a new phase in cooperation between authoritarian nation-states*. Russia, Iran, and North Korea are not just reimagined rogues of the international system but rather representatives of a new international order of non-democratic nations. Each of these states has close relations with Xi Jinping's People's Republic of China [3]. This is not a rehash of the Soviet Union's Warsaw Pact but rather a group of autocrat-led countries which stress and strain the diplomacy and military power of Western countries referred to by some as 'NATO Plus' (NATO+). What these four countries have been able to do is to sow chaos through the threat of force or its employment around the globe. The Russo-Ukraine War has shown that Vladimir Putin's regime has friends, and those friends are willing and able to aid in the war effort. Iran supplies the inexpensive drones blasting Ukraine's energy infrastructure. North Korea exports artillery ammunition. China cleared boycotted Russian oil exports from the global market, albeit at a substantial discount.

In the wake of Putin's grab for Ukraine, the authoritarian states identified here have been rhetorically cooperative, but to what degree have their cyber and information influence operations intersected? For example, China allegedly launches information influence campaigns against Taiwan [4], employing lessons learned by Russia and where Iran makes use of cyberattack knowledge from North Korea [5]. Beyond that, these countries lay underpinnings of challenges of the Western order they perceive as operating against their interests. Presented here are: (1) a framework for describing the linkages between these four states, both before and after the 2022 Ukraine invasion; (2) the *modus operandi* of cyberattack by each as well as an appraisal of recent (last 24 months) activity; and (3) description of information operations in the form of digital propaganda, and how those operations have evolved since Russia attempted to capture Kyiv and gain control over Ukraine.

2. Framework: Autocratic Alignment and the Russo-Ukrainian War

Russia's invasion of Ukraine across several axes on 24 February 2022 represented both major escalation of their conflict dating back to 2014 and dramatic change in the international system. Competition between major powers, set aside during the period of US hegemony for the prior three decades, was firmly reinitialised. This has triggered a reappraisal of theoretical models for understanding international relations and foreign policy [6]. At the core of this analysis resides the question of how strategic linkages between several autocratic states may arise. Central to this thesis is a reimagined Russia willing to scuttle relations with its Western economic partners and double down on its cooperation with other autocratic regimes. Like others in the international system, Russia seeks security, although of late it appears more inclined to destabilise other states and undermine its near-abroad neighbours.

Putin's Russia is part of just one traditional security pact, the Collective Security Treaty Organization (CSTO), which includes five other Soviet successor states. It also has many defence cooperation agreements (DCAs), which are 'formal bilateral agreements that establish institutional frameworks for routine defence cooperation' [7]. Russia maintains DCAs with no less than 20 countries across the Americas, Africa, Asia, and Europe, including ones with China, North Korea, and Iran. Finally, there is the Shanghai Cooperation Organization (SCO), which includes China, Iran, and Russia, but not North Korea.[1] It sends mercenaries to the Middle East and Africa; sells arms to dozens of nations; and appears willing to share technology with its closest allies.

The 2022 invasion of Ukraine has moved Russia to the status pariah state [8]. What does that mean? 'Pariah states are ostracized by significant portions of the international community for egregiously violating international norms'. Typically, they are governed by 'insecure authoritarian regimes' [9]. As a pariah state, Russia joins a growing list of others, including Myanmar, Venezuela, and Syria as well as Iran and North Korea. It is much larger than any of the others, and its future is largely dependent upon a linkage to China. 'For pariah states that flout international norms, China is a key

[1] The SCO also includes both India and Pakistan, nation-states with great enmity for each other.

source of diplomatic and economic support'. For Russia, China's support is embodied in the actions of an enabling sponsor which aids in evading sanctions, performs the role of a diplomatic shield, and engages in supporting information operations [10].

2.1. A Renewed Sino-Russian Alliance?

The closeness of collaboration between China and Russia rests upon how much they see themselves as aligned against the United States and how much Xi's China is willing to cooperate with heavily sanctioned pariah regimes. There are several metrics to consider in Sino-Russian cooperation. In the last decade, Xi Jinping and Vladimir Putin have met 42 times [11]. These meetings have occurred following the invasion of Ukraine, with a bilateral visit in Moscow in March 2023, followed by a sideline visit at the Third Belt and Road Forum in Beijing. Then there is trade. In 2023, the volume of trade between Russia and China hit a record high of $240.1 billion, marking a 26.3% increase from the previous year [12]. The volume of Russian oil exports to China rose by 24%, making it China's largest crude oil supplier, ahead of imports from Saudi Arabia [13].

There are also the words that unite the pair. In the joint declaration made weeks before Russia's Ukraine invasion, Xi and Putin indicated a deepening of ties. Their statement made at the opening ceremony of the XXIV Olympic Winter Games reaffirmed 'the new inter-State relations between Russia and China are superior to political and military alliances of the Cold War era', and that 'friendship between the two States has no limits' [14]. In a December 2022 call between Xi and Putin, Xi reiterated the need for, 'China and Russia to remain true to the original aspiration of cooperation, maintain strategic focus, [and] enhance strategic cooperation' [15]. More than two years into the Russo-Ukrainian War, Putin and Xi continue to celebrate 'deepened bilateral engagement and cooperation' between their countries [16].

2.2. What Role Theory?

As the international system migrates away from US hegemony to a new period of competition between major powers, there is also a need to reappraise approaches to understanding power in international relations. As was true on the eve of the Second World War, we can assume that power is wielded in three major areas: military, economic, and information [17]. China, Russia, North Korea, and Iran, the Big Four of major US adversaries, all engage in significant cyber and information operations. The question for the immediate future is how much these countries may cooperate in those operations. This requires an analysis of academic and trade cybersecurity sources as well as information operation trackers. That said, we require a theoretical overlay for understanding how the rogue regimes studied identify themselves as individual *and* collective actors. For this, we need a theoretic construct for understanding the roles that those states choose to play and how they prioritize those roles.

Holsti's groundbreaking work on state roles may serve as a beneficial heuristic device for understanding the foreign policy of pariah state cooperation [18]. While not a major plank of international relations, role theory can be a form of bootstrapping construct for understanding state behaviour. It 'offers a framework for describing national role performance and role conceptions and for exploring the sources of those role conceptions' [18]. Although more than five decades have passed since role theory came to foreign policy analysis, others have found it to have utility. Walker made use of role theory in much of his scholarship, including a contribution produced with Malici, highly relevant to this thesis on role theory and the behaviour of rogue states [19]. Thies and Breuning considered how it may be used to bridge study of foreign policy and international relations [20]. Cantir and Kaarbo employed it in understanding how domestic politics shape foreign policy roles [21].

While the role definitions that Holsti devised speak to the time of conceptualisation at the mid-point of the Cold War, we can consider the roles China and its pariah allies as contemporary analogues. Iran conceives of itself as both a 'defender of the faith' and 'regional leader'. North Korea may be the best described as an 'anti-imperialist agent' and a 'faithful ally' of China. Finally, Russia, the newest member of the pariah club, may see itself in the roles of regional leader and protector as well as an agent standing against the West. Goodness of fit of contemporary behaviour to mature theory is undoubtedly fraught with the potential for mischaracterisation, but the question at hand is how to place cyber and information operations into a conception of role.

How do we assign roles to understand cyber and information operations? That is the fodder for the following two sections. We must examine how these states behaved before 24 February 2022 as well as after this date. First to be treated is the milieu of cyberattack, which can be generally described as the subversion of systems regarding their maintenance of confidentiality, integrity, and availability [22]. This is an area in which each of the four countries studied definitely have developed clear behaviours that may translate to broader state roles.

3. Cyber Operations

Fancy Bear, *APT 28*, *Lazarus Group* – these are the code names given by the Western cybersecurity industry to different groups subverting online systems for political and military purposes, often as part of a criminal enterprise more lucrative than the drug trade. Since Russia's full-scale invasion of Ukraine in February 2022, some consider cyber conflict eclipsed by kinetic forms of warfare [23]. When we look at how the core members of the adversarial bloc use cyber techniques, there is little of the kinetic cyberattack activity of the sort perhaps feared most, but the employment of cyberattack remains an important tool for our four major adversary states.

North Korea robbed the accounts of a foreign central bank. Iran likely erased thousands of computer hard drives at Saudi Arabia's national oil company. Russia figured for attempting to destroy the computers used to operate portions of Ukraine's power grid. China was labelled the greatest thief of intellectual property by former secretary of defense and CIA director Leon Panetta [24]. While any country able and willing appears to be using cyber methods for intelligence gathering, each of the states covered here also use them for what would be economic espionage or criminal activity; things shunned in the West. Each of the four powers identified here has brought unique attributes to cyber campaigns. In its cyber offensive behaviour, North Korea is a cybercriminal gangster state. Iran is a theocratic warrior mixing the efforts of proxies with cyber operations to destabilise its enemies. Russia has performed masterful cyber-espionage campaigns while also crossing the Rubicon into effective acts of cyber-kinetic action. Finally, China has used cyber techniques to vacuum up enormous amounts of sensitive and proprietary data while attempting to steer global data flows to its purview for purposes of surveillance and potentially subversion.

3.1. A Record of Cyber Exploits in Brief

Before the invasion of Ukraine, North Korea, Iran, Russia, and China had highly visible cyberattack programs of concern to the United States and its allies. North Korea stands out for its gangsterism as well as criminal cleverness. Kim Jong-Un's cyber forces are a state criminal enterprise, and they are expert in theft. As of 2022, North Korean hackers had reputedly stolen some $1.5 billion in cryptocurrency from the wallets of unsuspecting virtual currency holders [25]. In February 2016, North Korean hackers attempted an enormous heist, attempting to lift nearly $1 billion from the Bangladeshi central bank's account at the New York Federal Reserve Bank. North Koreans are also behind a significant piece of the global ransomware racket, with the country's *Lazarus Group* behind the 2017 *WannaCry* ransom encryption software [26]. While WannaCry raked in very little, perhaps $1.5 million, the cost to organisations and individuals stricken by it amounted to billions, making it a significant disruptive attack [27]. In addition, *WanaCry* made use of source code from a cyber exploit know to and used by the US Intelligence Community. Other North Korean cyber actions have aimed more at disruption adversaries than anything else.

Where North Korea's cyber efforts are largely designed to fill the coffers of state and its ruling elite, Iran has employed forms of cyber action to pursue its political–ideological objectives [28]. Important in understanding Iran's own offensive cyber aims is the impact of *Stuxnet*, a series of cyberattacks upon the country's nuclear-enrichment infrastructure. Discovery of the *Stuxnet* software did allow Iran to engage in an interesting form of collaboration. While most of the detective work on *Stuxnet* was performed by cybersecurity firms and experts, further investigation of Iran's sensitive networks revealed the presence of other sophisticated malware created by what was labelled *The Equation Group*, a euphemism for the US National Security Agency. The malicious software, codenamed *Duqu* and *Flame*, were discovered in a shared effort undertaken by Russian cybersecurity firm *Kaspersky* in collaboration with Budapest University of Technology and Economics as well as the Iranian national computer emergency response team (CERT). Iran found the International Telecommunications Union (ITU) a helpful partner in bringing *Flame* out of the shadows. The ITU's then director, Hamadoun Touré, is a graduate of Soviet graduate institutions, and may have aided cooperation between the parties to a considerable extent [29]. By focusing on Iran's compromised systems, Russia likely gained deep knowledge of the US and likely Israeli cyber operations and tools. Months after discovering *Flame*, Iran ostensibly launched *Shamoon*, a data deletion attack against its neighbour Saudi Arabia, targeting the country's national oil company [30]. Was it helped by Russia? That is a question without a publicly known answer.

Moving along to Russia, the rump state of the former Soviet Union has a record of cyber operations stretching back to the massive virtual attack it conducted against Estonia in 2007 [31]. Moscow launched increasingly sophisticated cyberattacks on Ukraine after the country's leadership chose to forge closer ties with the West. Those attacks became increasingly menacing after Russia's proxy operations in the Donbas and later invasion of Crimea. The *Petya/Not Petya* wiper malware spilled beyond Ukrainian targets, damaging the IT systems of several major multinational firms [32]. It also took a page from the *Stuxnet* playbook in its attempt to knock offline Ukraine's *oblenegro* regional electricity distribution concerns. While largely unsuccessful, this last operation struck a nerve as the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, or GRU, demonstrated a significant capability in attacking industrial control system computers managing pieces of Ukraine's critical infrastructure [33]. Cyber operations, mostly designed to purloin sensitive information, were also a significant portion in Russia's information operations aimed at sowing chaos in the 2016 US national elections [34].

In stark contrast to Russia's disruptive operations, China's cyber activity has largely focused on one activity, espionage. China's cyber operations have vacuumed up massive amounts of information, largely in the areas of industrial espionage and the theft of intellectual property for both civilian and military development [35]. Google left China in 2010 over the theft of the firm's intellectual property via cyber means [36]. Chinese intelligence operatives penetrated the computer networks of the US Office of Personnel Management (OPM), the human resources office of the American government, and then proceeded to copy a massive volume of sensitive information on federal employees, including security clearance paperwork [37]. Elements of US weapons design have showed up repeatedly on Chinese platforms, indicating breaches at major defence contractors [38]. In addition to the collection of economic and military information, China has used cyber techniques for espionage directed at dissenters in its overseas diaspora, foreign diplomatic missions, and even the international organisations charged with regulating sport [39]. While often discovered in the act, China has remained undeterred in its massive cyber intelligence operation.

3.2. Activity in the Wake of the War(s)

How have the cyber operations of North Korea, Iran, Russia, and China changed in the last 2 years? To answer this, requires visits to the literature of cyberattack produced by cybersecurity companies, academics, and independent researchers. Ostensibly a failure of government in the United States and elsewhere, the cybersecurity industry provides an enormous amount of intelligence information regarding cyberattack techniques, hostile actors, and system vulnerabilities [40]. The actions of hostile states have evolved; however, each of the four countries studied appears to be sticking with its pre-2022 cyber operations gameplan. As the cybersecurity consultancy Crowdstrike demonstrates with its stockpile of incident response data (see Tab. 1), each of the four has largely stuck to its previously established pattern of attack behaviour.

That said, Iran's activity appears to have grown notably, not in the last 2 years, but more recently. Iran, once allegedly targeted by Israel for cyberattack, is increasingly turning the tables on it. Since the 7 October 2023 surprise attack by *Hamas* on Israeli territory adjacent to the Gaza Strip, Iran has dramatically increased its cyberattack activity. Operations include data leaks, data deletion, denial of service, and perhaps most menacing, threat of attack on critical infrastructure targets. Iran's cyber offensive capabilities are likely growing but examples of Iranian collaboration with other states remain few. In December 2023, Iran's legislature approved an agreement signed by the two countries' foreign ministers regarding cyber threats and information security [41]. Lopez-Rodriguez et al.

Table 1. Cyber activity by country, 2023.

Adversary group	Description
Russia	
Fancy Bear	Credential collection on MS-Exchange and phishing
Cozy Bear	Credential collection through MS Sharepoint and Office365
China	
Jackpot Panda	Malicious utility Trojan deployment
Cascade Panda	Actor-in-the-middle attacks & remote access tools (RAT)
North Korea	
Labyrinth Chollima	Supply chain compromise
Iran	
Spectral Kitten	Leaked PII, CCTV intrusions
Haywire Kitten	Cyber-kinetic attack threats, hack and leak ops, and distributed denial-of-service (DDoS)
Banished Kitten	Wiper data deletion attacks
Vengeful Kitten	Wiper and cellular infrastructure attacks

Source: Crowdstrike Global Threat Report 2024.

offer that both Russia and Iran have attacked energy infrastructure by cyber means but provide no evidence of collaboration in the wake of the Ukraine invasion [42]. Ties between Iran's increasing cyber attack profile and Russian support are rumoured, but thus far concrete evidence of those ties does not appear to have made it into open sources [43]. In messaging, however, there may be suggestions of greater closeness between China and its pariah allies.

4. Digital Propaganda

All four of the adversary states observed here have a two-fold information strategy. First and foremost, each maintains internal information controls on their populations [44]. To Western observers with relatively unfettered access to information, the internal information resources of Russia or China appear draconian. Regarding external information operations, the public messaging of state organs, especially Russia's, appear ludicrous. Of Ukraine, Russia's *Pravda* offers headlines like 'Zelensky's give-me-more-money ship is to sink at Davos' and 'Special military operation to end with Russia reuniting with Ukraine'. China's *People's Daily* suggests that American support for Ukraine equates to a message on how 'US pursuit of democracy puts world at risk'. Concern is that external propaganda strategies draw on this unreality to manipulate and subvert opinion in democratic states, in some cases with significant success. Internal and external information strategies of China and the pariahs combine unreality on both sides of the coin.

Internal controls on speech are common to the authoritarian regimes covered here. Massive powerful internal security forces are also common to all four countries. In Iran, its *Gast-e Ersad* or Guidance Patrol polices on violations of Islamic law while many of the other law enforcement agencies work to stifle counterrevolutionary activities [45]. North Korea also maintains an enormous, coercive internal security machine, which according to the US State Department human rights reporting may jail as many as 120,000 of the country's citizens [46]. Both Russia and China imprison political dissidents, protestors, and critics of their regimes. In both countries, dissidents frequently disappear, and China's government frequently purges government officials at the highest levels [47]. When former Chinese deputy leader Li Keqiang died in October 2023, aged 68, critics of the Chinese government wondered if his death by heart attack in a swimming pool was a euphemism as much as Russian deaths from falling out of windows [48].

With its massive information and computing technology (ICT) sector, China has thoroughly connected itself to the world's communications networks [49]. Conversely, access to the Internet in North Korea is highly restricted and limited primarily to government officials, select institutions, and a small number of foreigners living in the country. Most North Koreans do not have access to the global Internet, although some internal information technologies exist [50]. In between them reside Russia and Iran, both of which have purchased Chinese technologies that are part of its the so-called *Great Firewall* [51]. The *Great Firewall* is a sophisticated system for deep packet inspection and censorship of information access and communications [52]. In addition to blocking Internet traffic, China also employs a strategy to substitute Chinese-owned Internet platforms and tools for those owned by the US or Western firms. Facebook, Wikipedia, and X (formerly Twitter) are banned in China, and Internet searches are performed in compliance with China or not at all.

With the late 2021s, China brought its own applications to global audiences. In 2022, TikTok, a Chinese short-form video social media platform was again the most popular app download, globally, for mobile phones. This has drawn concern from Western governments [53]. TikTok is banned on the mobile devices of state employees in Texas, including the author. That said, the threat TikTok presents, other than to other forms of media, remains vague at best [54]. Other methods of Chinese propaganda range from state-run online news and entertainment to use of Western platforms for the placement of Chinese state messages and images [55]. Indeed, Chinese employment of social media in propaganda capitalizes on the US firms and their advertising business models [56].

It was Russia which showed how much the social media enterprise could be used to bring chaos to the lifeblood of the West's democratic governments, their elections. Nearly a decade after the US 2016 presidential election, considerable scholarship has been generated on how Russia employed social media to damage the political campaign of the candidate it found threatening, that of former senator and secretary of state Hillary Clinton [57]. Nadler et al. point out how the social media influencing technologies create a Digital Influence Machine (DIM), which can be employed, 'to identify and target weak points where groups and individuals are most vulnerable to strategic influence' [58]. As societies cultivated cultural and ideational influencers, Russian propagandists adapted their own influence techniques to this new, informational tableau for the purpose of achieving their external political goals. Zuboff's 'surveillance capitalism' had found a place in democratic politics [59]. The US social media firms were prepared to sell political advertising to firms they knew little or nothing about. Even worse, unlike traditional media, Facebook and Twitter held firm that they needn't label political advertising with the source of the ad.

While 2016 may represent the high-water mark for digital subversion of electoral processes through malicious employment of social media, its use has broadened and continuing. China has now gradually increased its use of social media disinformation strategies. During the recent 2024 Taiwanese elections, it on social media actively attempted to support its favourites and discredit candidates it views as threatening [60]. This was part of a coercive strategy that also includes military and economic planks for bringing Taiwan under increasing Chinese control and eventually unifying it with Beijing. At the same time, Russia continues to use DIM strategies to drive a wedge between Ukraine and her foreign allies as well as undermine democratic politics in those states it finds to be most threatening to its own geopolitical ambitions [61]. Iran too, actively engages in online disinformation campaigns, especially in support of its proxy operations in Lebanon, Syria, and Yemen [62].

In contemporary stocktaking, the pariah states may be able to significantly influence the politics of countries at a global distance. Moscow and Beijing's chief South American ally, Venezuela, has received strong informational support as its government postures to invade the oil-rich region of its neighbour Guyana [63]. Iran continues to produce propaganda in support of its Houthi and Hezbollah allies. For Russia and China, cooperation comes in the alignment of narratives and amplification of each other's messages, especially on platforms like Twitter and Weibo [64]. Chinese state-controlled outlets help spread the Kremlin's narrative of the war in Ukraine, often echoing Russian perspectives and criticisms of Western policies [65]. Additionally, both countries have targeted the Western financial system in their propaganda and disinformation campaigns. The collapse of Silicon Valley Bank in 2023, saw Russian and Chinese state media promoting narratives about the need for a new global financial system, often criticizing Western financial practices and institutions [66].

Iran presents again a novel picture for using the global information environment for its benefit. 'Iranian cyber actors have been at the forefront of cyber-enabled I[nformation] O[perations], in which they combine offensive cyber operations with multi-pronged influence operations to fuel geopolitical change in alignment with the regime's objectives' [67]. But again, Iran's actions in digital propaganda have a lot less to do with events in Ukraine than its own regional ambitions and willingness to use cyber, information, or proxy operations to erode the standing of Israel, the United States, and others involved in the region. Microsoft's reporting on Iranian information influence operations in the wake of the 7 October 2023 attacks indicates a four-prong strategy on undermining Israel. First, it is releasing propaganda designed to polarise the Israeli public, often masquerading as left-leaning Israeli voices. Second, it makes threats to Israeli infrastructure, even if those threats can't be made good. Third, it has used email and text messages to damage the morale of Israeli defence forces and their families. Lastly, Iran has attempted to undermine international support for Israel by amplifying images of destruction and privation in Gaza [68].

The great unknown for information influence at the time of writing is how China and each pariah state will act during the 2024 US general election. No doubt much will happen and digesting the true meaning and intention of those events. Information influence does not take place in a vacuum. The US and its allies continue to mobilise effort to better understand how influence operations work and also on how they may be short-circuited. Are China, Russia, Iran, and North Korea cooperating on information operations or is it just that their operations share the same targets. This we will continue to learn with additional time and data.

5. Conclusions

Collective security has been the cornerstone of the West's international security policy since 1945 [69]. During the Cold War, the members of the Warsaw Pact either feared invasion by or were indeed invaded by the Soviet Union. Just as suddenly as Soviet control extended across the territories it occupied in Europe's East during the end and immediate aftermath of the Second World War, the Soviet Union collapsed with only a Russian rump state (and its nuclear arsenal) remaining. More than 30 years later, Russia has found new expansionist ambitions played out in its near abroad, most notably in its invasion of Ukraine. It now sits at the centre of a security arrangement with North Korea and Iran, two-thirds of President George W. Bush's *axis of evil*. The full-scale war in Ukraine since 2022 has made Moscow an importer of arms from those two countries by sheer necessity. These both countries are also escalating their positions in regional conflicts and proxy wars to make the job of Western diplomacy and defence markedly harder. This stretches an American defence establishment thinner at a time when the maintenance of the US conventional deterrence appears more difficult [70].

Where that deterrence may be most important for the moment is in the Western Pacific. China's cyber and information operations indicate a growing impatience with Taiwan's independent status. Fortunately for Taiwan, cyber and information operations are far easier to undertake than kinetic military operations. The fundamental question to be answered from the conjectures offered here is to what degree China is part of the informal alliance between Russia, North Korea, and Iran [71]. If it is, then that makes the geopolitical stage all that more dangerous. That is because China brings an economic strength that the pariah states do not have. Time will tell if the adversarial bloc is real or if significant distance remains between China and the rest. For the American consumer, China is the manufacturer of their shoes, clothes, laptops, computers, and other consumer goods. For the US defense planner, it is the prime threat to Asian security and the justification for a 'pivot to Asia' that begun in the Obama administration [72]. Rectifying these realities into a workable strategic vision is vexing to say the least.

There are limits to cooperation. China and each of the pariahs has its own parochial interests. While evidence of an ideological break may exist between the West and China, this does not necessarily translate to a fundamental military or economic one. With many Western democracies still importing Russian oil and gas, Moscow has avoided a full economic disconnect from the rest of the world despite its invasion of Ukraine. For China, its bellicose language over Taiwan, maritime disputes, and other issues have not translated to a disconnection of its economy from the rest of the world either. If there is a lesson to be learned, it is that rhetoric in the channels of information power rarely matches willingness to engage in economic or military conflict. Talk remains cheap and the Internet makes transmitting it even cheaper.

Will China go it alone in meeting its objectives? Despite its now mature Belt and Road initiative, Chinese lending and infrastructure development has not yielded the form of security relationships coveted in Washington – 'The United States has fifty security pacts with different countries around the world. China has only one, with North Korea' [73]. If Russia, North Korea, and Iran are now China's allies, they make Beijing's designs on territorial aggrandizement in the South China Sea and absorption of Taiwan more achievable, simply by distracting the United States and its allies. Combined, these four nation-states can make much chaos in the information environment and cyber domain. They also can tie down NATO+ assets with the mere threat of military action. How well they will hang together and work collectively towards shared goals is perhaps the most pressing question in international security today.

References

[1] M. Kaczmarski, "The Sino-Russian relationship and the West," *Survival*, vol. 62, no. 6, pp. 199–212, Dec. 2020, doi: 10.1080/00396338.2020.1851101.

[2] T. Lattmann, "From partner to pariah: The changing position of Russia in terms of international law," in *Russia's Imperial Endeavor and Its Geopolitical Consequences: The Russia-Ukraine War*, Volume Two, B. Madlovics, B. Magyar, Eds., New York, NY: Central European University Press, 2023, pp. 183–198.

[3] L. Yu, S. Sui, "China-Russia military cooperation in the context of Sino-Russian strategic partnership," *Asia Europe Journal*, vol. 18, pp. 325–345, 2020, doi: 10.1007/s10308-019-00559-x.

[4] J. Lewis. (Aug. 11, 2023). *Cyberattack on civilian critical infrastructures in a Taiwan scenario*, Center for Strategic and International Studies. [Online]. Available: https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario. [Accessed: Dec. 7, 2023].

[5] S. Ragan. (Sep. 4, 2012). *Iran and North Korea Join Forces on Science and Technology*, *SecurityWeek*. [Online]. Available: https://www.securityweek.com/iran-and-north-korea-join-forces-science-and-technology. [Accessed: Nov. 03, 2023].

[6] A. Malici, S.G. Walker, *Role Theory and Role Conflict in US-Iran Relations: Enemies of Our Own Making.* Abingdon, Oxfordshire: Routledge, 2016.

[7] B. J. Kinne, "Defense cooperation agreements and the emergence of a global security network," *International Organization*, vol. 72, no. 4, pp. 799–837, 2018, doi: 10.1177/0022002719857796.

[8] K. Stoner, "The war in Ukraine: How Putin's war in Ukraine has ruined Russia," *Journal of Democracy*, vol. 33, no. 3, pp. 38–44, 2022, doi: 10.1353/jod.2022.0038.

[9] L.-E. Easley, J.T. Chow, "Enabling pariahs: China's support of Myanmar, North Korea, and Russia for geopolitical advantage," *Asian Survey*, vol. 64, no. 3, pp. 396–427, 2024, doi: 10.1525/as.2024.2113239

[10] J.T. Chow, L.-E. Easley, "Renegotiating pariah state partnerships: Why Myanmar and North Korea respond differently to Chinese influence," *Contemporary Security Policy*, vol. 40, no. 4, pp. 502–525, 2019, doi: 10.1080/13523260.2019.1660483.

[11] B. Lin, B. Hart, S. Lu, Y.-J. Liao. (Oct. 23, 2023.). *Analyzing the latest Xi-Putin meeting and China's belt and road forum*, Commentary, Center for Strategic & International Studies (CSIS). [Online]. Available: https://www.csis.org/analysis/analyzing-latest-xi-putin-meeting-and-chinas-belt-and-road-forum. [Accessed: Nov. 27,2023].

[12] Reuters. (Jan. 12, 2024.). *China-Russia 2023 trade value hits record high of $240 bln - Chinese customs*. [Online]. Available: https://www.reuters.com/markets/china-russia-2023-trade-value-hits-record-high-240-bln-chinese-customs-2024-01-12. [Accessed: Jun. 25, 2024].

[13] TASS Russian News Agency. (Jan. 19, 2024). *Russia exports record oil volume to China in 2023*. [Online]. Available: https://tass.com/economy/1734985. [Accessed: Jun. 25, 2024].

[14] President of Russia. (Feb. 4, 2022). *Joint statement of the Russian Federation and the People's Republic of China on the international relations entering a new era and the global sustainable development.* [Online]. Available: www.en.kremlin.ru. [Accessed: Nov. 27, 2023].

[15] R. Barrios, A. Bowen. (Sep. 13, 2023). *China-Russia relations*, Congressional Research Service, Washington, DC. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF12100. [Accessed: Nov. 27, 2023].

[16] W. Yang, "China, Russia double down on ties despite complications in trade relations," *Voice of America*, February 15, 2024.

[17] E.H. Carr, *The Twenty Years' Crisis, 1919-1939: Reissued with a New Preface from Michael Cox.* New York, NY: Springer, 2016.

[18] K.J. Holsti, "National role conceptions in the study of foreign policy," *International Studies Quarterly*, vol. 14, no. 3, pp. 233–309, 1970, doi: 10.2307/3013584.

[19] A. Malici, S.G. Walker, "Role theory and 'rogue states'," in *Deviance in International Relations: 'Rogue States' and International Security*. , W. Wagner, W. Werner, M. Onderco, Eds., London: Palgrave Macmillan, 2014, pp. 132–151.

[20] C.G. Thies, M. Breuning, "Integrating foreign policy analysis and international relations through role theory,"*Foreign Policy Analysis*, vol. 8, no. 1, pp. 1–4, 2012, doi: 10.1111/j.1743-8594.2011.00169.x

[21] C. Cantir, J. Kaarbo, "Contested roles and domestic politics: reflections on role theory in foreign policy analysis and IR theory," *Foreign Policy Analysis*, vol. 8, no. 1, pp. 5–24, 2012, doi: 10.1111/j.1743-8594.2011.00156.x

[22] O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, "The law of cyber-attack," *California Law Review*, vol. 100, pp. 817, 2012.

[23] E. Roche, M. Blaine, "The folly of cyber war," *Journal of International Affairs*, vol. 75, no. 2, pp. 131–144, 2023.

[24] L. Panetta, B. Obama, *Sustaining US Global Leadership: Priorities for 21st Century Defense.* Washington, DC: US Department of Defense, vol. 1, p. 16, 2012.

[25] During a track two visit by North Korean diplomats to Syracuse University in 2000, the chief of the delegation asked the author several questions suggesting fairly strong knowledge of software design and computer coding: J. S. Wit. (2019). "U.S. strategy towards North Korea: Rebuilding dialogue and engagement". [Online]. Available: https://usakoreainstitute.org/wp-content/uploads/2010/02/NKreportOCT09jwit.pdf. [Accessed: Nov. 27, 2023].

[26] A. Greenberg, "North Korean hackers stole nearly $400 million in crypto last year," *Wired*, Jan. 13, 2022. [Online]. Available: https://www.wired.com/story/north-korea-cryptocurrency-theft-ethereum. [Accessed: Oct. 10, 2023].

[27] S. Mohurle, M. Patil, "A brief study of wanna cry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017, doi: 10.26483/ijarcs.v8i5.4021.

[28] Web Titan. (Jul. 2, 2020). *How much money did wanna cry make?* [Online]. Available: https://www.webtitan.com/blog/how-much-money-did-wannacry-make. [Accessed: Dec. 03, 2023].

[29] G. Siboni, L. Abramski, G. Sapir, "Iran's activity in cyberspace: Identifying patterns and understanding the strategy," *Cyber, Intelligence, and Security*, vol. 4, no. 1, pp. 21–40, 2020.

[30] C. Bronk, "Cyber intrigue: The flame malware international politics," Cyber Dialogue, University of Toronto, May 31, 2012. [Online]. Available: https://cyberdialogue.ca/2012/05/cyber-intrigue-the-flame-malware-international-politics/. [Accessed: Nov. 03, 2023].

[31] C. Bronk, E. Tikk-Ringas, "The cyber attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013, doi: 10.1080/00396338.2013.784468.

[32] C. Bronk, "Hacking the nation-state: Security, information technology and policies of assurance," *Information Security Journal: A Global Perspective*, vol. 17, no. 3, pp. 132–142, 2008, doi: 10.1080/19393550802178565.

[33] A. Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired*, Aug. 22, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world. [Accessed: Nov. 27, 2023].

[34] R. Lee, M.J. Assante, T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, no. 388, pp. 1–29, 2016.

[35] C.E. Ziegler, "International dimensions of electoral processes: Russia, the USA, and the 2016 elections," *International Politics*, vol. 55, no. 5, pp. 557–574, 2018, doi: 10.1057/s41311-017-0113-1.

[36] N. Inkster, "Cyber espionage," *Adelphi Series*, vol. 55, no. 456, pp. 51–82, 2015, doi: 10.1080/19445571.2015.1181443.

[37] S.J. Hartnett, "Google and the 'twisted cyber spy' affair: US–Chinese communication in an age of globalization," *Quarterly Journal of Speech*, vol. 97, no. 4, pp. 411–434, 2011, doi: 10.1080/00335630.2011.608705.

[38] S. Gootman, "OPM hack: The most dangerous threat to the federal government today," *Journal of Applied Security Research*, vol. 11, no. 4, pp. 517–525, 2016, doi: 10.1080/19361610.2016.1211876.

[39] A. Gilli, M. Gilli, "Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," *International Security*, vol. 43, no. 3, pp. 141–189, 2018, doi: 10.1162/isec_a_00337.

[40] R. Deibert, R. Rohozinski, A. Manchanda, N. Villeneuve, G. Walton, *Tracking Ghostnet: Investigating a Cyber Espionage Network*. Toronto: Citizen Lab, University of Toronto, 2009.

[41] J.D. Work, "Private actors and the intelligence contest in cyber conflict," in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, R. Chesney, M. Smeets, Eds., Georgetown University Press, 2023.

[42] G. López-Rodríguez, I. Moreno-López, J.C. Hernández-Gutiérrez, "Cyberwarfare against critical infrastructures: Russia and Iran in the gray zone," *Applied*

Cybersecurity & Internet Governance, vol. 2, no. 1, pp. 1–7, 2023, doi: 10.60097/ACIG/162865.

[43] Iran International. (Dec. 10, 2023). *Iranian parliament approves information security deal with Russia.* [Online]. Available: https://www.iranintl.com/en/202312105187. [Accessed: Nov. 27, 2023].

[44] A. Davidi, "Iranian-Russian cooperation on hack attacks may challenge Israeli cyber supremacy," *The Times of Israel*, April 18, 2023.

[45] V. Weber, "The worldwide web of Chinese and Russian information controls," Oxford: Center for Technology and Global Affairs, University of Oxford, 2019. [Online]. Available: https://www.ctga.ox.ac.uk/article/worldwide-web-chinese-and-russian-information-controls. [Accessed: Jun. 25, 2024].

[46] S. Golkar, "The evolution of Iran's police forces and social control in the Islamic Republic," *Middle East Brief*, no. 120, vol. 3, pp. 1–9, 2018.

[47] K.C. Lee, "In the Kim Jong Un era what is the reality of social control and punishment in North Korea," *Korea Institute for National Unification*, 2023. [Online]. Available: https://repo.kinu.or.kr/handle/2015.oak/14464. [Accessed: Jun. 25, 2024].

[48] C. Chen, "What is behind anti-corruption? A comparison of Russia and China," *Communist and Post-Communist Studies*, vol. 53, no. 4, pp. 155–176, 2020, https://doi.org/10.1525/j.postcomstud.2020.53.4.155.

[49] K. Nakazawa. (Nov. 2, 2023). *Analysis: The mysteries and dangers that trail Li Keqiang's death*, Nikkei Asia. [Online]. Available: https://asia.nikkei.com/Editor-s-Picks/China-up-close/Analysis-The-mysteries-and-dangers-that-trail-Li-Keqiang-s-death [Accessed: Oct. 10, 2023].

[50] Y. Hong, G. T. Goodnight, "How to think about cyber sovereignty: the case of China," in *Norm Diffusion Beyond the West*, Š. Kolmašová, Ed. Springer Nature Switzerland, 2020, pp. 8–26.

[51] S.-A. Kim, C.Y. Kang, J. Park, B.Y. Yoon, *A Study on the Access to Information of the North Korean People*. Korea Institute for National Unification, 2021.

[52] S. Kalathil, *Beyond the Great Firewall: How China Became a Global Information Power*. Washington, DC: Center for International Media Assistance, 2017.

[53] E. Quan, "Censorship sensing: The capabilities and implications of China's great firewall under Xi Jinping," *Sigma: Journal of Political and International Studies*, vol. 39, no. 1, p. 4, 2022.

[54] A. Law, "The 'legal black hole' CFIUS and the implications of Trump's executive order against TikTok," *Cornell JL & Pub. Pol'y*, vol. 31, p. 217, 2021, doi: 10.59015/wlr.ACHH7075.

[55] M.L. Mueller, K. Farhat, "Regulation of platform market access by the United States and China: Neo-mercantilism in digital services," *Policy & Internet*, vol. 14, no. 2, pp. 348–367, 2022, doi: 10.1002/poi3.305.

[56] B. Min, L.R. Luqiu, "How propaganda techniques leverage their advantages: A cross-national study of the effects of Chinese international propaganda on the US and South Korean audiences," *Political Communication*, vol. 38, no. 3, pp. 305–325, 2021, doi: 10.1080/10584609.2020.1763524.

[57] J. Bund, *Finding China's Edge: Engineering Influence Operations within the Limits of Social Media Platform Rules*. ETH Zurich, 2021.

[58] Y. Golovchenko, C. Buntain, G. Eady, M.A. Brown, J.A. Tucker, "Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US presidential election," *The International Journal of Press/Politics*, vol. 25, no. 3, pp. 357–389, 2020, doi: 10.1177/19401612209126.

[59] A. Nadler, M. Crain, J. Donovan. (2018). *Weaponizing the digital influence machine*. [Online]. Available: https://datasociety.net/library/weaponizing-the-digital-influence-machine. [Accessed: Nov. 27, 2023].

[60] S. Zuboff, "The age of surveillance capitalism," in *Social Theory Re-Wired*, W. Longhofer, D. Winchester, Eds.,Abingdon, Oxfordshire: Routledge, 2023, pp. 203–213.

[61] H.-C. H. Chang, A. H.-E. Wang, Y. S. Fang. (2023). *US-Sskepticism: Misinformation and transnational conspiracy in the 2024 Taiwanese presidential elections*, Center for Open Science, [Online]. Available: https://misinforeview.hks.harvard.edu/article/us-skepticism-and-transnational-conspiracy-in-the-2024-taiwanese-presidential-election/. [Accessed: Nov. 27, 2023].

[62] L. Maschmeyer, A. Abrahams, P. Pomerantsev, V. Yermolenko, "Donetsk don't tell – 'hybrid war' in Ukraine and the limits of social media influence operations," *Journal of Information Technology & Politics*, pp. 1–16, 2023, doi: 10.1080/19331681.2023.2211969.

[63] H. Kermani, "#MahsaAmini: Iranian Twitter activism in the times of computational propaganda," *Social Movement Studies*, 2023, doi: 10.1080/14742837.2023.2180354

[64] R. Padula, M. de Freitas Cecílio, I. Candido de Oliveira, C.J. Prado, "Guyana: Oil, internal disputes, the USA and Venezuela," *Contexto Internacional*, vol. 45, 2023. [Online]. Available: https://www.scielo.br/j/cint/a/vTqm4rBBDg6WRMt3NyLyKtF/?format=pdf&lang=en. [Accessed: Jun. 25, 2024].

[65] S. Bendett, E. Kania. (2019). *A new Sino-Russian high-tech partnership," Australian Strategic Policy Institute*. [Online]. Available: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership. [Accessed: Nov. 27, 2023].

[66] J. Bodnar, B. Schafer, E. Soula. (2023). *A Year of Disinformation: Russia and China's Influence Campaigns During the War in Ukraine*, Alliance for Securing Democracy. [Online]. Available: https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/ [Accessed: Dec. 03, 2023].

[67] K. Walter, H. Hariharan, "China, Russia target western financial system with propaganda and disinformation," *The Diplomat*, Jul. 14, 2023. [Online]. Available: https://thediplomat.com/2023/07/china-russia-target-western-financial-system-with-propaganda-and-disinformation. [Accessed: Nov. 03, 2023].

[68] C. Watts. (May 2, 2023). *Rinse and repeat: Iran accelerates its cyber influence operations worldwide*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat. [Accessed: Nov. 03, 2023].

[69] C. Watts. (Feb. 6, 2024.). *Iran accelerates cyber ops against Israel from chaotic start*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel. [Accessed: Nov. 03, 2023].

[70] Charles. A. Kupchan, Clifford. A. Kupchan, "The promise of collective security," *International Security*, vol. 20, no. 1, pp. 52–61, 1995.

[71] E.D. Borghard, S.W. Lonergan, "Deterrence by denial in cyber-space," *Journal of Strategic Studies*, vol. 46, no. 3, pp. 534–569, 2023, doi: 10.1080/01402390.2021.1944856.

[72] N. Grajewski, "An illusory entente: The myth of a Russia-China-Iran 'axis'," *Asian Affairs*, vol. 53, no. 1, pp. 164–183, 2022, doi: 10.1080/03068374.2022.2029076.

[73] K.M. Campbell, R. Doshi, "How America can shore up Asian order," *Foreign Affairs*, vol. 12, 2021. [Online]. Available: https://www.foreignaffairs.com/articles/united-states/2021-01-12/how-america-can-shore-asian-order. [Accessed: Jun. 25, 2024].

[74] D. Singh. (Jan. 18, 2024). *Déjà new: A return to the old normal. Security, economics, and technology for Houston Llecture*, University of Houston. [Online]. Available: https://www.law.uh.edu/ipil/2024_SETH_Lecture_Series_photos.asp. [Accessed: Nov. 27, 2023].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Understanding Estonia's Cyber Support for Ukraine: Building Resilience, Not Status

Matthew Crandall | School of Governance, Law, and Society, Tallinn University, Tallinn, Estonia | ORCID: 0009-0000-2588-009X

Abstract

This article explores Estonia's cyber support for Ukraine following Russia's invasion in February 2022. Despite its small size, Estonia has significant cyber expertise and has played a pivotal role in safeguarding Ukrainian digital infrastructure and providing cybersecurity support. While Estonian cyber contributions to Ukraine are significant, it initially did not seek or receive international attention. Estonia is typically vocal in promoting its cybersecurity and e-governance expertise. This article aims to first explore the impact of Estonia's cyber support for Ukraine. Second, it aims to understand why Estonia did not try to use this support to bolster its status as a cyber authority. To do this, Estonia's cyber support is analysed and put into the proper geopolitical context. Interviews with high-ranking Estonian officials were conducted and an analysis of policy output was performed. This article finds that the importance of cybersecurity assistance is not as critical as military assistance, which is one reason why Estonia has not (yet) used its cyber assistance as a status opportunity. Although cybersecurity support may be considered secondary to military support, the significance of Estonia's cybersecurity assistance should not be overlooked. Although Estonia did not pursue status initially, there are some signs that this is beginning to change and Estonia is recognised for its cyber expertise.

Received: 03.01.2024

Accepted: 30.05.2024

Published: 05.07.2024

Cite this article as:
M. Crandall, "Understanding Estonia's cyber support for Ukraine: Building resilience, not status," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190396

Corresponding author:
Matthew Crandall, School of Governance, Law, and Society, Tallinn University, Tallinn, Estonia; E-mail: crandall@tlu.ee
0009-0000-2588-009X

Keywords

cybersecurity, Ukraine, resilience, status

1. Introduction

Russia's invasion of Ukraine on 24 February 2022 is seen in Estonia as an existential threat. Ukraine's importance to Estonia started long before the invasion in 2022 or the illegal annexation of Crimea in 2014. Estonia has long prioritised Eastern partnership countries, Ukraine, Moldova, and Georgia in particular, in development cooperation and foreign policy priorities [1]. In the lead-up to the 2022 invasion, Estonia's support for Ukraine was significant. Military assistance was the most attention-getting aspect of assistance. For example, Estonia provided Javelin anti-tank missile systems and decided to provide 122 mm artillery systems before the invasion began [2]. After the start of invasion, Estonia has been among the most vocal in its support for Ukraine. This was particularly evident when looking at military aid as a percentage of GDP; Estonia was among the top donor countries. In addition to military support, Estonia has been active in providing both military and civilian cyber support. Estonia's cyber support has not received noteworthy attention within Estonia or internationally. This is a stark contrast to the attention Estonia has received for the level of military and political support for Ukraine. For example, in April 2023, President Volodymyr Zelensky in a meeting with Estonian Prime Minister Kaja Kallas said: 'If every leader and every state were equally conscientious about protecting our common freedom on the continent, Russia's aggression would have already been defeated without question' [3]. What makes this development striking is Estonia's past promotion of its cyber expertise [4]. Given Estonia's internationally recognised cyber expertise and its promotion of itself as a cyber authority, it is surprising that it would not have brought more attention to its cyber support for Ukraine. This article explores the cyber assistance Estonia has provided to Ukraine and why Estonia has not yet tried to leverage this support to bolster its status as a cyber expert.

Estonia's cyber support for Ukraine merits a closer analysis for several reasons. First is the nature of the war in Ukraine. This is the first large-scale, long-term war involving a developed country dependent on the Internet [5]. The implications of this are significant. This changes both nature and importance of cybersecurity. Second, what impact can a small state with limited resources have on cybersecurity assistance? It is one thing for a small state to emphasise cyber support as part of a development cooperation strategy during a time of peace, and it is another to react in a crisis.

Smaller states typically have limited material resources and thus cannot influence international affairs with military and economic might. Although there are exceptions like Israel or Norway, those are not reflective of the position of most small states. A majority of small states tend to pursue normative change and influence international affairs through avenues that do not require excessive resources [6]. One typical way is to be a standard bearer. Modelling ideal behaviour can be used as an example for other states. This is, perhaps why status-seeking is an appropriate conceptual framework to understand small state behaviour. Estonia, like many small states, has pursued a strategy of status-seeking. In particular, Estonia has modelled itself as an expert in cybersecurity and e-governance, adopting the nickname e-Estonia [4]. Given Estonia's significant cyber support for Ukraine, it is peculiar that Estonia has not publicly tried to boost its status as part of its strategy of cyber assistance. For example, the Ministry of Foreign Affairs page on support for Ukraine details a long list of different ways Estonia has supported Ukraine and Ukrainians. There is virtually no mention of any cyber support, aside from a list of donated goods that mentions IT equipment [2].

To better understand this paradox, this article first maps out Estonia's cyber support for Ukraine and place it in a larger geopolitical context. It then explores the reasons, why Estonia has not used this support to boost its own status. To do this, government documents and publications were analysed. In addition, expert interviews were conducted. This article then proceeded with a discussion on methods and a conceptual framework of status-seeking. This follows with two analytical sections, one mapping out Estonia's support for Ukraine, and another discussing the impact of the strategy and how the strategy was influenced by geopolitical considerations. The article concludes with implications of what this all means for small states with high cyber aspirations.

2. Literature Review: Small State Status in Cyberspace

Status in international relations is an emerging concept that is used to understand the foreign policy of aspiring great powers as well as small states. Status has its theoretical origins in a theory from psychology, the Social Identity Theory developed by Tajfel and Turner [7]. In this theory, the key to understanding individuals is the relationship between groups and group membership. There is a need for positive self-esteem, which happens from inter-group comparisons. Status is then a social hierarchy that can be best understood when group interactions are taken into consideration [8]. There are many authors who applied this concept of psychology to international relations. Paul et al. discussed in their 2014 edited volume status in international relations [9]. The influential volume focused on emerging states and rising powers. The pursuit of status is not just for large states. As Neumann and Carvalho note, small states do not have the luxury of pursuing the power game or investing in tools of coercion due to limited resources [10]. Small states then must rely on moral authority for their pursuit of status [10]. In many ways, status as a theoretical concept is even more applicable for small states as most small states face status uncertainty [10]. This concern is also evident in the small state literature on ontological security. It has been argued that states suffering trauma are more prone to status uncertainty [11]. Estonia and other states occupied by the Soviet Union would fit this profile. There have been quite a few authors that have looked at small states seeking status in recent years. Most authors looked at single-state case studies, such as Cyprus [12], Lithuania [13], and Estonia [1], as well as others.

Status can be sought out for multiple reasons. For some, status can be the means to justify an end, thus a state would seek status to have a better chance at pursuing its foreign policy interests [14]. For others, the pursuit of status is the end goal due to the above-mentioned status uncertainty that small states often face. No matter the goal, looking at inner and outer group dynamics is key to understanding any status-seeking behaviour. Small states usually seek status from great powers by proving their usefulness [10]. There are also opportunities for small states to seek status from those outside their own status group [15]. The relationships of status-seeking can vary. In addition to states, international organisations are also an important avenue to seek status. The nature of status-seeking means that most status-seeking endeavours are highly visible campaigns and developments. Depending on the circumstances, status-seeking could be more targeted and remain outside the public eye. Small states and the United Nations (UN) Security Council can demonstrate this process [16]. For example, Estonia's selection to the UN Security Council from 2020–2021 was a visible act of status-seeking that included a global campaign and a successful vote in the UN General Assembly. Estonia's work on the UN Security Council was not as visible to the public but also resulted in an increase in status and improved reputation from other states who were serving with Estonia on the UN Security Council [17].

Despite the increasing literature on small-state status-seeking behaviour, there is no clear picture of the conditions that shape small-state status-seeking strategies. Why would a state choose a certain relationship or campaign to improve its status? The focus of this article is on Estonia and its cybersecurity assistance to Ukraine, from 24 February 2022 to the end of 2023. Looking at this relationship, it sheds light on the conditions needed for a state to seek out status.

At first glance, Estonia has not been as vocal in drawing attention to its cyber support for Ukraine, instead it focused on its military contributions. This seems at odds with the long-standing strategy of status-seeking via cybersecurity and e-governance. To better understand this development, the article uses a mixed methods approach utilising desk research and document analysis. Primary sources were gathered from government documents and strategies mostly produced by the Estonian Ministry of Foreign Affairs specific to Estonia’s support for Ukraine. Estonia, like many other states, includes NGOs in the implementation of policies, especially in development cooperation. Regarding cyber assistance and Ukraine, a key institution is and has been the e-Governance Academy. Project information and documents related to Estonia’s cyber assistance to Ukraine were analysed. In addition, two expert interviews were conducted in Tallinn, one in the late summer of 2023 and another in December 2023. Both high-ranking officials had intimate experience and knowledge of Estonia’s cyber assistance to Ukraine and Estonia’s strategy regarding cyber diplomacy foreign policy priorities. Due to the sensitive nature of the interviews, the officials desired to remain anonymous. This also ensured responses that are more direct. The officials were from different government institutions and complemented each other with their experiences. The identity of the officials, the transcripts of the interviews, and confirmation that the interviews took place, were shared with the editorial board to ensure that the rigours of academic research were met. The thoughts and takeaways from this article are heavily influenced by these interviews and the officials’ perspectives.

The article analyses the data in two sections: first, a section outlining Estonia’s cyber support to Ukraine, and second, the implications of Estonia’s support and a discussion of its impact (or lack thereof) on Estonia’s status-seeking strategy.

3. Estonian Support for Ukraine

One of the key elements of Estonia’s foreign policy has been to increase its status within key international frameworks, such as North Atlantic Treaty Organisation (NATO) and the European Union (EU) [18]. Estonia has tried to be a model ally, a producer of security, not only a consumer of security [19]. Although Estonia has done much to enhance its status in many aspects, it is the most visible in terms of cybersecurity and e-governance [20]. Estonian leaders share a consensus about the importance of developing and maintaining cyber and e-governance competencies. Estonia has developed innovative e-governance services that are international attention-getters, such as online voting and an e-residence program [21]. Perhaps, the most effective framework Estonia has used to increase its status has been NATO. Tallinn is the location of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). The CCDCOE facilitated the Tallinn Manual I and II, describing how international law can apply to cyberspace. The Tallinn Manual I and II bear the name of Tallinn, which put Tallinn in 'the mental world map of international law with a purposefully accomplished project' [22].

Russia's war in Ukraine brought large-scale World War II-style military conflict back to the heart of Europe. However, Ukraine is an advanced society with many digital services and dependencies on connectivity [23]. This created a significant challenge for Ukraine and for those assisting Ukraine to help keep Ukraine online. Russia's invasion of Ukraine changed the nature and scope of Estonia's cyber support for Ukraine. The following information is based on the expert interviews unless cited otherwise. The opinions of both expert interviews have been combined to allow this section to have a thematic flow.

Estonia's cyber support to Ukraine goes back well before the 2022 invasion. Cooperation in improving information and communication technologies (ICT) and e-governance solutions has been the backbone of Estonia's development cooperation strategy for some time now [18]. The e-Governance Academy has been the primary organisation to implement development cooperation projects. Projects carried out in Ukraine currently listed on their website go back to 2014 and cover several topics such as boosting e-governance solutions, improving cybersecurity readiness in Ukrainian public officials, and building cyber defence capabilities. The cost of the projects ranged from €44,000 to more than €17 million [24]. The funding often comes through EU funding mechanisms.

Having connections with Ukraine before the war broke out made it easier for Estonia to provide support after the war began. A few days before the war broke out, a team of Estonian cybersecurity officials travelled to Ukraine to meet their counterparts to establish person-to-person contact. At that time, it was not completely sure as to what would happen, but things were pointing towards a war. These contacts were beneficial in helping to coordinate support after the breakout of the war.

Estonia's cyber support to Ukraine can be divided into two aspects: practical support and diplomatic support. Practical support can be largely described as bilateral cooperation. One key area of practical assistance Estonia provided was help safeguarding Ukrainian digital infrastructure. Ukraine needed to evacuate a significant amount of its public digital infrastructure, which was not an easy task. For many services, this meant relocating to the cloud, but due to the specific hardware of some systems, not everything could be deployed in the cloud. Some systems were exported to NATO territories to be maintained as an operational service. Estonia's attitude towards cyber assistance was to help in any way that Estonia could. As one official put it, 'Any assistance Ukraine wanted, if we were able to provide it we did, without hesitation'. Most of the support Estonia provided was intangible support, such as putting data in safekeeping and getting servers up and running.

Both officials interviewed stressed the important role of coordination in the support that Estonia gave. The outbreak of the war was described as a nightmare, a mess, and there was a lack of consolidation on Ukraine's part. Ukraine was understandably focused on the military aspect of defence and the intensity of the cyberattacks were at their highest before the invasion began. Requests for assistance were going from multiple channels to multiple actors and the result was confusion. Western partners had to know what Ukraine needed to avoid duplication and ensure that Ukraine could absorb the assistance. Estonia's prior contacts with Ukraine enabled Estonia to play a key role in helping to streamline the coordination efforts.

The key to shoring up and enabling Ukrainian cyber defence was the implementation of Western tech, usually from the private sector. One obstacle Ukraine faced with this was export controls and getting a licence for the product or service. In this situation, Estonia was able to relay requests to the US State Department, validate requests made by Ukraine, and play a constructive role in helping to get information to the proper actors promptly.

Perhaps, the most significant and certainly visible outcome of Estonia's cyber support for Ukraine is the Tallinn Mechanism, which was launched on 20 December 2023. This mechanism systematises support from various countries and companies for civilian cyber assistance to Ukraine [25]. Estonia has assigned a diplomat to Kyiv to support the mechanism and has earmarked Euros 500,000 from its development cooperation fund to support the Tallinn Mechanism and Ukrainian civilian cybersecurity assistance. The participating countries, in addition to Estonia, are Canada, Denmark, France, Germany, The Netherlands, Poland, Sweden, the United Kingdom, and the United States. Given the long-term attacks and threats Ukraine is and will be facing from Russia, the Tallinn Mechanism aims to replace the ad hoc nature of cyber assistance with a systematised and more coherent manner. Estonia hopes that this format could be a model for future conflicts. The Tallinn Mechanism works in tandem with the IT coalition, which coordinates cyber assistance for military means.

Estonia is also a founding member of the IT coalition along with Ukraine and Luxembourg [26]. This is a good example of Estonia taking the initiative and making a difference. At a meeting of IT Coalition, Ukrainian minister of Defence Rustem Umerov stated that 'Technology will win the war … our advantage will be provided by asymmetric responses and they are possible, thanks to innovations that are already working' [27].

The second aspect of Estonian cyber support to Ukraine is diplomatic support. Diplomatic support happened in both open- and closed-door settings. Estonia has often supported Ukraine in the UN's open-ended working group on the use of ICT. Estonia promotes the application of international law in cyberspace and responsible behaviour in cyberspace [28]. Russia's actions in Ukraine go against both of these principles. Estonia has also consulted Ukraine on boosting its cyber diplomacy capabilities to improve its influence in the UN and globally.

Estonian diplomatic support also took place behind closed doors. Two instances are worth noting that were highlighted by the experts. In the early stages of the war, Estonia offered one platform so that Ukraine could exchange information securely. Some EU partners were vocal in their concern for this move because they also used the same platform. There was concern about the potential risk to them. Estonian officials spent a significant amount of time discussing and alleviating those concerns. In another format with multiple countries, the topic was raised to donate dual-use software. It was designed to detect vulnerabilities to improve cyber defence, but it could also be used to find vulnerabilities in Russia's systems and be used as an offensive capability. Estonia has for years argued against the myth of offensive cyber capabilities. As one official noted, self-defence in cyberspace includes the use of offensive cyber capabilities. Estonian officials advocated for Ukraine and were a voice of reason: if bombs and guns were already being provided, then a piece of dual-use software would not change the risk factor for EU countries. The process was slow and Ukraine's request was eventually filled.

Although Estonia is a small state with limited resources and a country that does not have big technology companies, the contributions to helping Ukraine with cyber support were significant and noteworthy. When one official was asked if they were satisfied with Estonia's cyber support to Ukraine, the answer was yes. This still begs the question, if Estonia's contribution was significant, then why would Estonia not use this to improve its status as an expert in cybersecurity and e-governance? Why would Estonia not promote itself as a standard bearer for others to follow suit? The next section tackles these questions and discusses the implications and limitations of Estonia's cyber support.

4. Building Resilience Now, Status Later

Estonia's support for Ukraine should not be trivialised. One of the most sobering points raised by an official was how often Estonia was attacked by a distributed denial-of-service (DDoS) attack after Estonian state leaders made any public comment critical of Russia. This works like clockwork. Why then, despite the effort, the cost, and the risk is Estonia's cybersecurity support not talked about more? There are several reasons noted by the officials interviewed. As one official noted, 'Ukraine will not win the war with their e-solutions. Russians can be beaten right now by brutal force'. In this conflict we are not seeing cyberattacks against hospitals, we are seeing bombs hitting hospitals. What Ukraine needs the most is military support. This explains why Estonia has emphasised so heavily the need to do more to militarily support for Ukraine and why Estonia has emphasised itself as a standard bearer of military support to Ukraine as opposed to cybersecurity assistance.

A secondary concern is also related to risk management involved. Estonia needs to be cautious with what is supplied to not draw undue attention and increase its odds of being a target. The nature of Estonian cyber support was different from military support. Where military support was delivering material products to Ukraine, cyber support meant hosting Ukrainian data and servers in Estonia and facilitating Ukrainian communication with Estonian tools.

This invites a larger discussion about the nature of cyber capabilities in conflict. Some reflections on this topic have been already drawn [29]. As noted in the publication, cyber operations did not yield strategic results. One of the Estonian officials speculated that it also was related to Russia's miscalculations about how it would be a short war. This meant that after the initial cyberattacks before the war began, they took a back seat to the military invasion. Yet, we should be weary of treating these as separate. Cyber is linked to military capabilities, especially with intelligence. Cyber operations have played a significant role in disinformation campaigns and promoting narratives and messaging.

Many works on small states tend to overestimate the impact that a small state causes. It is important to mention the limitations of Estonia's support to Ukraine. The real hero in Ukraine's cyber defensive resilience is the Western technologies that Ukraine is using. The question was once asked how big is a small state in cyberspace (personal communication with peer reviewer on a draft version of an article, 2015)? It turns out that in a time of war the small state still has limitations due to a lack of resources. However, this does not mean that a small state cannot make a difference. Indeed, Estonia is hopeful that the collective response to provide cyber assistance to Ukraine can be a model for future conflicts.

What might all this mean for Estonia's status as a cybersecurity expert and an expert in e-governance? As one official stated, 'We will probably hear more about this in the future'. The official continued that the war is an existential threat to Estonia. Thus, we can see that status does not serve a primary function. When the existential threat has been subdued, then we can assume that Estonia will return to a more typical foreign policy of status-seeking. Some level of status-seeking has already taken place. The Tallinn Mechanism bears the name of Tallinn, similar to the Tallinn manuals, which is a good first step to ensuring that Estonia is internationally recognised for its effective cyber assistance to Ukraine.

5. Conclusions

This article observed Estonia's cyber support to Ukraine. Estonia, as a small state and a recognised cybersecurity expert, presented an interesting subject. Typical small-state behaviour would suggest that small states would seek status, something Estonia has consistently done by promoting itself as a cybersecurity expert. This article explored why Estonia's cyber support to Ukraine has not been used to build status. It found that for Estonia, the aftermath of the invasion was not the time or place to pursue a status-seeking policy. Risk factors and more important priorities left cyber assistance out of the public eye. As the chaos of the invasion eased, Estonia eventually began to pursue a more typical status-seeking policy. This was most evident with the creation of the Tallinn Mechanism. Estonia's cyber support to Ukraine is significant in terms of both practical support and diplomatic support. The creation of IT Coalition and Tallinn Mechanism are significant and tangible accomplishments for Estonia. Owing to long-standing cooperation before the conflict, Estonia was more effective in playing the role of a facilitator. Although this might not seem like something significant, Estonia helped to solve the largest problem at the beginning of the war, that is, bringing structured coordination to a scene of chaos.

The nature of the conflict is such that military capabilities determine the outcome of the war. Accordingly, Estonia has focussed its messaging efforts on its military support for Ukraine and drawing attention to the importance of continued allied military support for Ukraine. If there is room for status-seeking, then it is not be at the expense of military support for Ukraine. While cyber operations have not been the defining feature of this war, it has still caused more questions to be asked.

While the focus of this paper is on a small state supporting Ukraine, there were other questions raised in the interviews, such as the role of big tech in conflicts. For a small state, this creates more questions and potential vulnerabilities when a CEO can make decisions that influence a conflict. Since cyber operations did not have a determining impact in this conflict, will this lead to a lack of attention for cyber defence capabilities and best practices? Perhaps the biggest takeaway for Estonia is that this has not been a one-way relationship. Estonia has been in close dialogue and learning from Ukraine's experiences as well. During this time of crisis, we can see that Estonia's key strategy is to help Ukraine win the war and also to help Ukraine and Estonia develop cyber resiliencies to be ready for future crises.

References

[1] V. Made, “Shining in Brussels? The Eastern partnership in Estonia's foreign policy,” *New Perspectives,* vol. 19, no. 2, pp. 67–80, 2011.

[2] Estonian Ministry of Foreign Affairs. (May 31, 2023). *Estonia's aid to Ukraine*. [Online]. Available: https://vm.ee/en/estonias-aid-ukraine [Accessed: Aug. 20, 2023].

[3] The Kyiv Independent. (Apr. 24, 2023). *Zelensky meets with Estonian prime minister in Zhytomyr Oblast*. [Online]. Available: https://kyivindependent.com/zelensky-meets-with-estonian-prime-minister-in-zhytomyr-oblast/. [Accessed: Mar. 30, 2024].

[4] A. Papp-Váry, "A successful example of complex country branding: The 'e-Estonia' positioning concept and its relation to the presidency of the council of the EU," *Acta Universitatis Sapientiae, European and Regional Studies*, vol. 14, pp. 87–115, 2018, doi: 10.2478/auseur-2018-0013.

[5] M. Crandall, Anonymous high-ranking Estonian official, personal communication, Tallinn, Dec 28, 2023.

[6] G. Magnúsdóttir, B. Þórhallsson, "The Nordic States and agenda-setting in the European Union: How do small states score?," *Icelandic Review of Politics and Administration*, vol. 7, no. 1, pp. 205–225, 2011, doi: 10.13177/irpa.a.2011.7.1.11

[7] H. Tajfel, J.C. Turner, "An integrative theory of intergroup conflict,"in *Monterey*, W.G. Austin, S. Worchel, Eds., Pacific Grove, CA: Brooks/Cole, 1979, pp. 33–37.

[8] J.C. Turner, "Towards a cognitive redefinition of the social group," in *Social identity and intergroup relations*, H. Tajfel, Ed., Cambridge: Cambridge University Press, 1982, pp. 15–40.

[9] T.V. Paul, W.D. Larson, W.C. Wohlforth, *Status in world politic*s. New York, NY: Cambridge University Press, 2014.

[10] I.B. Neumann, B. de Carvalho, Eds. "Introduction: Small states and status," in *Small state status seeking: Norway's quest for international standing*. London: Routledge, 2014, pp. 1–15.

[11] P. Charoenvattananukul, *Ontological security and status-seeking: Thailand's proactive behaviours during the Second World War*. New York, NY: Routledge, 2020.

[12] R. Pedi, K. Chainoglou, "The Republic of Cyprus in international and regional organizations: Towards a mature small state status seeking strategy?" in *The foreign policy of the Republic of Cyprus: Local, regional and international dimensions*, Z. Tziarras, Ed. Cham: Springer, 2022, pp. 287–309.

[13] A. Park, G. Jakstaite-Confortola, "Small state status-seeking: Lithuania's foreign policy status aspirations," *Europe-Asia Studies*, vol. 73, no. 7, pp. 1279–1302, 2021, doi: 10.1080/09668136.2021.1919291.

[14] R. Pedi, I. Kouskouvelis, "Cyprus in the Eastern Mediterranean: A small state seeking for status," in *The new eastern Mediterranean*, L. Spyridon, A.Tziampiris, Eds., New York, NY: Springer, 2019, pp. 151–167.

[15] M. Crandall, M.L. Sulg, "Small states and new status opportunities: Estonia's foreign policy towards Africa," *European Politics and Society*, vol. 24, no. 2, pp. 250–264, 2021, doi: 10.1080/23745118.2021.1990662.

[16] B. Thorhallsson, A.M. Eggertsdóttir, "Small states in the UN security council: Austria's quest to maintain status," *The Hague Journal of Diplomacy*, vol. 16, no. 1, pp. 53–81, 2020, doi: 10.1163/1871191X-BJA10017.

[17] R. Nodapera, *Small states in the UN security council: Case of Estonia through two presidencies in May 2020 and June 2021.* Master's thesis, School of Governance, Law and Society, Tallinn University, Tallinn, 2021.

[18] M. Crandall, I. Varov, "Developing status as a small state: Estonia's foreign aid strategy," *East European Politics*, vol. 32, no. 4, pp. 405–425, 2016, doi: 10.1080/21599165.2016.1221817.

[19] T.H. Ilves. (Dec. 5, 1996). *Address by foreign minister Toomas Hendrik Ilves to the Riigikogu*. [Online]. Available: https://vm.ee/en/news/address-foreign-minister-toomas-hendrik-ilves-riigikogu [Accessed: Aug. 20, 2023].

[20] M. Crandall, C. Allan, "Small states and big ideas: Estonia's battle for cybersecurity norms," *Contemporary Security Policy*, vol. 36, no. 2, pp. 346–368, 2015, doi: 10.1080/13523260.2015.1061765.

[21] M. Kimmo, I. Pappel, D. Draheim, "E-residency as a nation branding case," in *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, A. Kankanhalli, A. Ojo, D. Soares, Eds., New York, New York, USA, 2018, pp. 419–428.

[22] L. Mälksoo. (Aug. 8, 2013). *The Tallinn manual as an international event*. [Online]. Available: https://icds.ee/en/the-tallinn-manual-as-an-international-event. [Accessed: Dec. 30, 2023].

[23] F. Plantera. (2021). *The path towards e-Governance in Ukraine*. [Online]. Available: https://ega.ee/success_story/path-towards-egovernance-ukraine. [Accessed: Dec. 30, 2023].

[24] e-Governance Academy. (2023). *Digital transformation for Ukraine (DT4UA) projects*. [Online]. Available: https://ega.ee/projects/?country=ukraine. [Accessed: Dec. 30, 2023].

[25] Estonian Ministry of Foreign Affairs. (Dec.12, 2023). *Tallinn Mechanism*. [Online]. Available: https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism [Accessed: Dec. 22, 2023].

[26] Estonian Ministry of Defence. (Sep. 19, 2023). *Estonia, Luxembourg and Ukraine launched an IT coalition to support Ukraine*. [Online]. Available: https://www.kaitseministeerium.ee/en/news/estonia-luxembourg-and-ukraine-launched-it-coalition-support-ukraine. [Accessed: Dec. 30, 2023].

[27] Interfax Ukraine. (Nov. 29, 2023). *Umerov to participants of IT coalition: Technology to win war*. [Online]. Available: https://en.interfax.com.ua/news/general/950946.html. [Accessed: Dec. 30, 2023].

[28] Estonian Ministry of Foreign Affairs. (2021). *Estonian contribution on the subject of how international law applies to the use of information and communication technologies by states, to be annexed to the group of government experts on advancing responsible state behavior in cyberspace (2019–2021).* [Online]. Available: https://www.vm.ee/media/799/download on 30.12.2023. [Accessed: Dec. 30, 2023].

[29] M. Schulze, M. Kerttunen, "Cyber operations in Russia's war against Ukraine," *SWP Comment*, no. 23, p. 8, Apr 17, 2023, doi: 10.18449/2023C23.

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Cyber Influence Defence: Applying the DISARM Framework to a Cognitive Hacking Case from the Romanian Digital Space

Alina Bârgăoanu | Faculty of Communication and Public Relations, National University of Political Studies and Public Administration, Bucharest, Romania | ORCID: 0000-0003-3912-8442

Mihaela Pană | National University of Political Studies and Public Administration, Bucharest, Romania

Abstract

One of the main lessons learned in the context of Russia's full-scale invasion of Ukraine starting in February 2022 is that foreign information manipulation and interference (FIMI) operations are closely coupled with cyber threats. Regardless of whether cyberattacks are followed by an information manipulation component and vice versa, the merger of the two can be an early indicator of the potential for a conflict to escalate from the cyber area to the ground. Our article is premised on the idea that today's highly technologised information ecosystem is a fertile ground for cyberattacks and information manipulation in the context of FIMI; more specifically, it enables cognitive hacking, meaning hacking the human mind and human cognition altogether through technological disruption and cyber pressure. Starting from this premise, the aim of the article is to highlight the technological determinants of cognitive hacking and identify silent or emerging threats that bypass technological sensors and seek to disrupt and manipulate the information environment. The empirical part is based

Received: 26.03.2024

Accepted: 02.06.2024

Published: 10.07.2024

Cite this article as:
A. Bârgăoanu, M. Pană "Cyber influence defence: Applying the DISARM framework to a cognitive hacking case from the Romanian digital space," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190196

Corresponding author:
Alina Bârgăoanu, Faculty of Communication and Public Relations, National University of Political Studies and Public Administration, Bucharest, Romania; E-Mail: alina.bargaoanu@comunicare.ro
0000-0003-3912-8442

on observation as a descriptive method, which is used to analyse a case of cognitive hacking carried out via a YouTube malvertising campaign targeting Romanian users. This case study is analysed qualitatively by matching the DISinformation Analysis & Risk Management (DISARM) framework with evidence collected through Open-Source Intelligence (OSINT) tools, following an innovative analysis structured according to the purposes, actions, results and techniques (PART) model. The extensive analysis of the identified case shows that applying the DISARM framework to cyber-enabled operations can be useful for anticipating and responding to FIMI threats, even when such operations do not appear to have a specific, immediately identifiable purpose.

Keywords

cognitive hacking, FIMI, cyberattacks, cyfluence, deepfake, OSINT analysis, DISARM framework, malvertising

1. Introduction

After the COVID-19 pandemic and the accompanying infodemic, humanity reached a flashpoint with two simultaneous geopolitical conflicts that present the potential to disrupt the current world order. Analyses of the events of the last 4 years converge on the thesis that the cognitive dimension has become a new frontier of offensive and defensive military actions. Russia’s full-scale invasion of its neighbouring country, Ukraine, coupled with the conflict between Hamas and Israel following the 7 October 2023 terror attacks, led to the new hybrid threat architecture, at the heart of which lies the battle for peoples’ minds, enabled by our dependence on technological structures. In this turbulent context, the threat of cyber influence could be disguised as a regular cyber-crime that bypassed technology filters silently and crosses all the adversary lines.

Given the immaterial environment of the human mind, where the effects of hostile actions can only be inferred from people’s perceptions, decisions and behaviours, how can cyber interference be proved? Does technology provide the same conditions to track attackers through digital fingerprints and build a behavioural profile to determine the threats against which to protect oneself? The answers to these questions form the basis of this research, which lies at the intersection of information security and communication studies.

To exemplify the theory of cognitive warfare conducted by combining information operations with cyberattacks to enhance psychological effects, the objective of this paper is to describe and analyse a cognitive hacking case using multiple tools and methods, with the aim of consolidating the practice of hybrid threat-integrated anticipation and response. Specifically, by observing two inauthentic video ads on YouTube targeting Romanian users, this paper analyses how deepfake videos, fabricated content and compromised websites are blended together to deliberately spread false information and malware. This case study provides insight into the hybrid approach needed to effectively manage a hybrid threat, such as cognitive hacking, using open-source tools and an innovative strategic analysis framework.

The case study findings lead to the analysis of cognitive hacking by tracking disinformation and malvertising – a method used to describe misleading ads that contain malicious code or redirect users to malicious websites [1, 2]. This case study reveals how to use Open-Source Intelligence (OSINT) for evidence-gathering in the attribution of hostile actions and how to apply the DISinformation Analysis & Risk Management (DISARM) framework to cyber-enabled influence campaigns for anticipating foreign information manipulation and interference (FIMI) operations, even when such operations do not appear to have a specific, immediate identifiable purpose.

1.1 Cognitive Hacking in the Context of the Russia–Ukraine Cyber War

A good understanding of cognitive hacking is related to the large picture of Russian cyber operations aimed at extensively disabling Ukraine's critical national infrastructure [3], telecommunications, banking, transport, water supply and energy supplies [4] during the past 10 years. This concept emerged at the disruptive cyberattacks of the first major crisis in Eastern Europe, the pro-European protests in Ukraine that took place in 2013 under the name EuroMaidan [5], and grew intensively before and after the armed conflict triggered by Russia in Ukraine [6–8], shifting to the human cognitive dimension as a new type of critical national infrastructure [9]. Weaponising the online manipulation capabilities of new technologies [10] and exploiting human addiction to social media, the weak control mechanism of the distribution of online content and undetected technical vulnerabilities create the premises for cognitive warfare [11–13].

1.2 Cognitive Warfare: From Cyber-Enabled Influence to Cyfluence and Cognitive Hacking

From a technological perspective, both humans and information systems can be viewed as the endpoints of information exchanges [14]. According to Cybenko's early research, if influence operations are deliberate activities targeting the cognitive dimension with the aim of changing the attitude or behaviour of the target audience, as Hollis concluded [15], cognitive hacking refers to a computer or information system attack that relies on changing human users' perceptions and corresponding behaviours to be successful [16]. In NATO's approach, cognitive warfare integrates cyber, information, psychological and social engineering capabilities. These activities, carried out in conjunction with other instruments of power, can affect attitudes and behaviour by influencing, protecting or disrupting individual and group cognition to gain advantage over an adversary [17]. New and emerging technologies, such as artificial intelligence (AI) and deepfake, combined with disinformation, microtargeting and algorithmic echo chambers reveal the future of hybrid threats [18].

Seen as a 'strategy that focuses on altering how a target population thinks and through that how it acts' by Backes and Swab [19] and 'the weaponization of public opinion, by an external entity, for the purpose of influencing public and governmental policy and destabilizing public institutions' in Bernal et al.'s findings [20], cognitive warfare is determined by at least two essential components: *cognitive domain operations* (CDOs), which use emerging technologies to advance battles into 'the realm of the human mind' [21], and coordinated chaos [22], which synchronises cyberattacks and disinformation to manufacture crises and disrupt public responses as a 'never-ending battle for minds' [23].

In line with the latest research findings, the approach of treating the cognitive dimension as an offensive and defensive manoeuver space has emerged from the US military [9]. The analysis of Russia's actions over the past 10 years, culminating with the outbreak of a full-scale military invasion in February 2022, reveals the hybrid nature of offensive and defensive actions and the integration of technology in attempts to destroy or weaken the adversary from a cognitive point of view [24, 25].

While analysing the fusion between hostile influence campaigns, cybersecurity and AI, Yonat points out that 'the attackers are light years ahead of us and moving faster than us'. He explains 'cyfluence' as a concept used to define the embedding of cyberattacks in influence campaigns [26]. He also highlights the cataclysmic effect of using AI in influence operations, ‘not just damaging companies or individuals or just harming countries; it is literally tearing apart societies, bringing down democracies, taking humanity one enormous step toward another dark age’ [26].

The contemporary information ecosystem has created ‘the worst cognitive warfare conditions since WWII’ [27], affecting a nation’s cognitive infrastructure, which Gourley described for the first time as ‘the mental capacities of the citizens and the decision-making ability of people, organisations, and our government’ [28]. Regarding responses to this new type of threat, the Swedish approach appears to be the most advanced model. Established in 2021, the Swedish Psychological Defense Agency, organised as a government agency under the Ministry of Defense, is in charge of identifying, analysing and countering foreign malign information-influenced activities [29].

1.3 Convergence between Disinformation, Influence and Cyberattacks

The concept of cyber pressure can be related to the increasing number and sophistication of cyberattacks [30], hybridisation of attackers’ motivations and techniques, increased risk of an unknown vulnerability being exploited without any possibility of knowing it, lack of adequate cyber threat anticipation as a result of poor technological knowledge, and poor resource allocation under time pressure, technological illiteracy among users, poor communication skills of technical specialists, the speed of technological transformation, and an unpredictable and unstable geopolitical environment. Given this pressure, cyberattacks have become part of the ecosystem of disinformation operations [31, p. 9], which is why the cyber risk associated with this threat is considered at all levels, from business [32] to national security [33].

The hybridisation of attacks by combining cyber and information warfare to create social harm has a new pattern: cyberattacks are used as a tool for information attacks, and information attacks are used to amplify the alleged success rate of cyberattacks. Both seek to strain people’s trust in public action and public entities, create a general sense of insecurity, and erode the capacity to act and react under crisis situations. ‘[Distributed denial-of-service] DDoS attacks and defacement erode people’s trust in their institutions and their ability to protect their own population’ [34].

Covert cyber operations are carried out through techniques and tactics, such as social engineering, phishing campaigns, the penetration and capture of computer systems, and the development and control of troll and bot farms. Hacking computer systems to extract documents, publishing illegally accessed documents in truncated or altered versions, capturing legitimate email or social media accounts to disseminate false information, and penetrating content management systems of official websites to spread influence narratives are part of the arsenal of techniques used in cyber influence operations [35, pp. 120–124].

Misinformation and disinformation are recognised among the security threats included in the official analysis of European Union (EU) [36], in direct association with the notion of attempts to influence human behaviour. Furthermore, the European Cyber Security Agency (ENISA) report states that these two threats have become the core of cybercrime activities, which have led to the emergence of the Disinformation-as-a-Service (DaaS) business model. The EU Cybersecurity Strategy [37] also states that hybrid threats combine disinformation campaigns with cyberattacks on infrastructure, economic processes and democratic institutions, with the potential to cause material damage, facilitate illegal access to personal data, facilitate the theft of industrial or state secrets, sow distrust, and weaken social cohesion.

If the main objectives of hybrid warfare are to take control of society, influence people’s cognition and disrupt decision-making processes, as well as to gain access to a country’s strategic, communication and critical infrastructures by effectively combining soft and hard power [38], then the ability to weaponise new technologies attracts the attention of entities interested in global domination or at least disruption of cyberspace. Researchers have identified the emergence of online influence operations since 2004. As states have shown interest in online influence using microtargeting [39, p. 47], the phenomena of fake news, misinformation and disinformation have become serious challenges to modern society [40]. Consequently, the covert use of social media by promoting propaganda, advocating controversial and toxic narratives, playing both sides of highly divisive issues, and spreading misinformation have become common tools [41].

Analysing how different state actors deployed cyber tools and tactics for hybrid warfare during a major crisis over the past decade, Duggan [42, p. 47] described the ‘synchronized choreography’ between disinformation and cyberattacks, which can help people gain time and space for conventional military forces. The ability to penetrate the computer systems of individuals, organisations and institutions significantly increases the potential for effective disinformation and propaganda delivered through both traditional and unconventional means. Thus, cyber actions can increase the potential of influence operations and enrich the information content available to information warfare operators. Cyberscale operations also have socio-psychological effects on citizens and security institutions by distracting attention from the broader manifestations of information warfare [43, 44, p. 12].

The toolkit of hostile actions enabled by the highly technologised cyber environment has grown in variety and sophistication: false information, hyper-partisan content, disinformation, impersonation, false identities, trolls or bot farms, deepfakes, cheapfakes, hacking, hijacking, disconnecting or destroying mobile devices, stealing sensitive information, and leaking personal data. All these hostile actions are encompassed under umbrella concepts, such as cyber-enabled foreign interference [45] or cyber-enabled information warfare and influence operations [46], associated with tools of hybrid interference [47] or forms of hybrid warfare [48].

Zurko, a cybersecurity researcher at MIT Lincoln Laboratory, argues that

> in cybersecurity, attackers use people as a means to undermine a technical system. Disinformation campaigns are designed to impact human decision-making; they are the ultimate use of cyber technology to undermine people. (…) Both use cyber technology and people to achieve a goal. Only the goal is different. Just like cyberattacks, influence operations often follow a multistep path, called a kill chain, to exploit predictable weaknesses [49].

For this reason, Lincoln Lab's efforts are focused on '*source tending*' as well as strengthening the early stages in the kill chain to find new countermeasures for disinformation campaigns.

The ENISA and the European External Action Service (EEAS) have underlined the link between disinformation and cyberattacks and focused on the concept of FIMI. This concept is included in the cybersecurity threat landscape [50] and is used to describe a largely non-illegal pattern of behaviour that threatens or has the potential to negatively impact political values, procedures and processes. Such activity is manipulative in nature and carried out in an intentional and coordinated manner. Additionally, the misinfosec conceptualised by

Walker [51] brings forth the idea of using an information warfare kill chain to understand cyber-enabled influence operations. For this reason, the DISARM framework [52] organises ways of describing and analysing disinformation, covering intent to deceive, intent to harm, and coordinated inauthentic behaviour.

Developed based on cybersecurity best practices, the DISARM framework is designed to gain a common understanding of digital disinformation. The project was designed to codify and share intelligence on disinformation and influence operations through a knowledge base of techniques and countermeasures and presented as a standard that the EU and the United States are now using to analyse and share information in countering FIMI threats [53].

The DISARM phases refer to the highest-level grouping of tactics and their associated techniques, corresponding to a specific time interval in the execution of an influence campaign [54]. If a tactic reveals the adversary's goal for each stage, the techniques lead the way in which the goal is achieved. The kill chain represents the minimum number of steps required for a successful attack. A broken link results in a failed attack, which is beyond the scope of tagging research. Following the DISARM approach, this paper tests the frameworks to identify a case of cognitive hacking from a cyber-enabled influence campaign [55].

2. Methodology

Building upon this conceptual framework, we delve into a detailed examination of a malvertising campaign to investigate how advertising platforms can be utilised for cognitive hacking. To accomplish this goal, our case analysis demonstrate the utility of open-source information in identifying the tactics, techniques, and procedures (TTPs) employed in a cognitive hacking campaign and how these can be matched within the DISARM framework to counter FIMI operations.

The empirical part is based on a case study as a descriptive method that allows for a detailed understanding of a particular case. The analysis is focused on YouTube advertising campaigns targeting Romanian users by showing how deepfake videos, fake news, and compromised websites are blended to deliberately spread false information and malware.

The cognitive hacking case was first spotted on YouTube in May 2023, running in two YouTube video ads about some benefits for vulnerable social groups without specifying who offers them and under what conditions they can be obtained. The obvious pattern of misleading based on inauthentic content suggests that a large-scale malicious campaign that needs to be captured and investigated before any efforts are made to remove it from the online space. For further reference to this case, we call it YouTube_benefits_Ro.

For this case analysis, the research strategy involves five steps: case identification, message analysis, digital analysis, and OSINT analysis – to track digital fingerprints and collect evidence of misleading actions following an innovative strategic analysis structure by proposing the purpose, actions, results, and techniques (PART) model. Tagging the technological determinants of cognitive hacking into the DISARM framework contribute to a better understanding of the behavioural profile of this case. The research stages were as follows (Fig. 1):

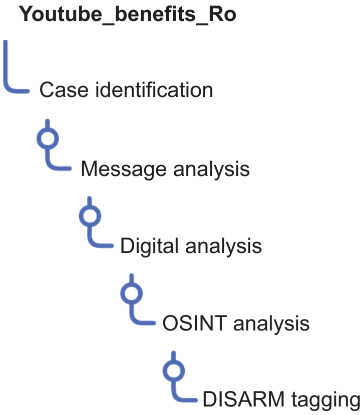


Figure 1. The research stages.

1. Case identification – capture the facts when they happen
2. Message analysis – follow the model of the structured analytic framework based on Lasswell's communication formula
3. Digital analysis – gathering elements related to identified facts
4. OSINT analysis for tracking FIMI fingerprints – collect evidence of misleading actions following the PART model strategy
5. Tagging TTPs into the DISARM framework – version 1.3

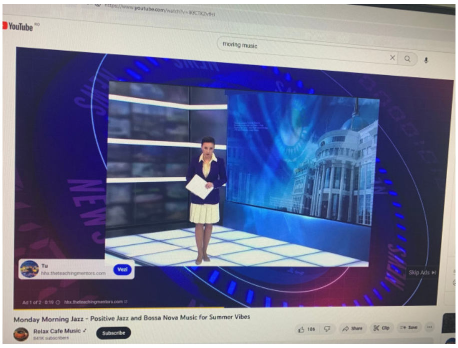
3. Research Results

3.1. Case Identification

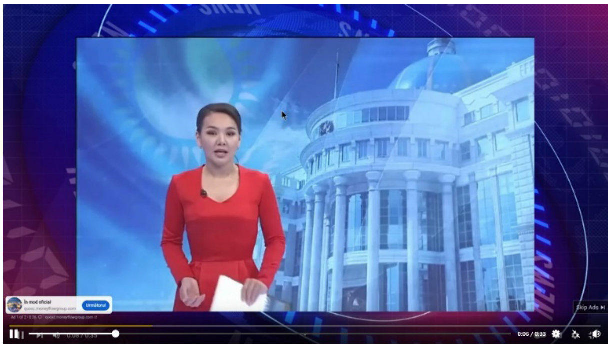
Video ads targeting vulnerable social groups in Romania were observed when accessing YouTube by nonpaid users in

May 2023. Using a fabricated news flash, an unknown TV presenter announced new benefits of between €5,000 and €10,000 for vulnerable people without mentioning any real recognisable Romanian entity. The targeted audience was mentioned in the second sentence of the message: 'The retired people, pregnant women, low-income people, people with disabilities and many other categories', usually associated with vulnerable social groups with poor cyber hygiene or media literacy to be aware of cyber threats or influence activities. Another misleading clue was the domain of the website mentioned in the video ad, which was redirected to another website.

The high level of uncertainty, an unidentifiable entity, an inauthentic figure, irrelevant visual elements for the audience, and redirection to some subdomains of foreign sites were the triggers to capture this piece of deliberate mislead as it was unfolding and to start the analysis. After refreshing the same page, another video ad stood out, with another presenter and another website related to the ad, but with the same message and the same visual elements.


https://www.youtube.com/watch?v=IKfCTKZvfHI
YouTube RO
moring music
NEWS
Tu
hhx.theteachingmentors.com
Vezi
Skip Ads
Ad 1 of 2 · 0:19 hhx.theteachingmentors.com
Monday Morning Jazz - Positive Jazz and Bossa Nova Music for Summer Vibes
Relax Cafe Music
841K subscribers
Subscribe
106
Share
Clip
Save

First capture of the video ad on YouTube



Second capture of the video ad on YouTube

Photo of the video ads on YouTube (ANNEX 1).

After capturing the website and the video, the case was reported to the Romanian National Cyber Security Directorate as an instance of misleading content related to compromised websites. As a result, the sites mentioned above were blocked from being accessed from Romania immediately after that notice.

3.2 Message Analysis

The message analysis follows the model of the structured analytic framework based on Lasswell's communication formula for providing an understanding of the influencing attempts [56, p. 5]. The message was composed of seven short sentences with many unspecified details and unidentified entities expressing supportive behaviour in a polite manner. The only precise elements were the audience – 'retired people, pregnant women, low-income people, people with disabilities and many other categories', the value of benefits – 'planned to be between 5,000 and 10,000 Euro per person', and the call to access the news website (Table 1).

Table 1. The message structure of the video ad promoted on YouTube.

1. Starting this Monday, (unintelligible) introduces benefits for several categories of citizens.
2. Retired people, pregnant women, people on low incomes, people with disabilities and many others will receive benefits.
3. The benefits are planned to be between 5,000 and 10,000 Euro per person.
4. More information can be found on our news website.
5. The method to get the benefits is simple and anyone can do it.
6. You can also read more interesting news.
7. Have a nice day!

3.3. Digital Analysis

The digital analysis is based on public information included in websites promoted in YouTube ads, hhx.theteachingmentors.com and gute.mycalculat.com, to determine as much information as possible about the entity behind the ad campaign and the promoted sites. To perform digital analysis, four actions (A) were carried out.

The first action (**A1**) involved searching the YouTube ad transparency database by website name using the https://adstransparency.google.com/?region=RO tool. The search indicated that the Google Ads Transparency Center has no public evidence of this video advertising campaign, even though it had been active for at least 3 weeks.

The second action (**A2**) involved checking the websites mentioned in the video ad: hhx.theteachingmentors.com and gute.mycalculat.com. The findings indicate that the websites have the same sitemap: the homepage, one article, and the policy page. There are no active links from homepage to article page, only sensitive images (namely, visualisations of older people in poverty, mentioning safety retirement income, and social security reform) and click bait titles redirected to homepage. All the websites share the same web design, sitemap, and policy page, which is an indication of mass-created websites and a clue that helps to detect and block scam websites used by masquerading attacks. The sites under analysis appeared to be compromised by attackers, as indicated by the fact that they displayed error pages or bad connections during the analysis.

During the third action (**A3**), we checked the content of the websites hhx.theteachingmentors.com and gute.mycalculat.com. There was no information about the data, authors, contacts, or copyrights that could be linked to a real identity.

Finally, the fourth action (**A4**) involved checking the policy page found at hhx.theteachingmentors.com and gute.mycalculat.com. The website privacy policy mentions the Russian Federal Law on Personal Data No. 152 FZ, suggesting that the section is copied from a Russian website. Additionally, this page mentions the name Mihailov Ivan Sergheevici as a data operator (screenshots of the digital analysis are displayed in ANNEX 2). This final evidence helped to discover other websites used in this cognitive hacking campaign during the OSINT analysis stage.

3.4. OSINT Analysis

To perform OSINT analysis for tracking fingerprints and gathering evidence of misleading and harmful actions, we structured the research steps according to the PART model strategy that can be replicated in future OSINT analyses.

The PART model organises the actions (**A**) around the main purposes (**P**) using different OSINT tools for each purpose. The results (**R**) reveal evidence of misleading and harmful actions that can be associated with tactics, techniques, and procedures – TTPs (**T**) – or indicate new directions for analysis purposes. Furthermore, the

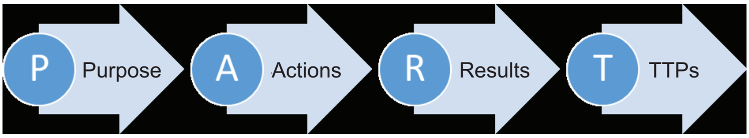


Figure 2. Illustration of the PART model for OSINT analysis of cognitive hacking, as proposed by the authors during the research.

identified TTPs can be correlated with indicators from other databases, such as the DISARM framework, which is described in the next section of the research. Screenshots of the OSINT results are shown in ANNEX 3.

The first purpose (**P1**) was to check for additional information about the websites to which the campaign was leading by performing the domain name search in search engines (**A1**). The Google search results led to one more video ad recorded by a Reddit user (**R1**) that included the essential element – the original YouTube channel that managed the video ad campaign – which has an anonymous and generic name (**T1**): '*România astăzi*' (Romania Today) @romaniaastazi-zl2pj and the evidence of using fake news planted on a newsfeed website weeklynewsfeed.com (**R2**). The fake article planted on weeklynewsfeed.com mixed false information with excerpts copied from an authentic news website (**T2**), including real names of several public officials talking about the Student Invest and Family Start social funding programs and loan facilities of up to €10,000 with interest paid in full by the state. The second video captured by the other Reddit user leads to another website domain name: quoxc.moneyflowgroup.com (**R3**). The analysis revealed that hiding fabricated news in an anonymous newsfeed service is an information laundering technique.

The second purpose (**P2**) was to check the authenticity of the visual content. The video footage shows an official building leading up to an authority representation. Google image identification (**A2**) matches this image with the Ak Orda Presidential Palace in Kazakhstan (**R4**). The correlation of the presenter's physiognomy with the lack of coherence between facial gestures and speech in Romania indicated the use of an AI-generated voice-over for a stock video (**T3**). For this reason, we checked the video with deepfakedetector.ai (**A3**). The result shows a very high probability of deepfake content (**T4**): 71.19% (**R5**).

To complete the third purpose, we checked for any YouTube-related information (**P3**) by performing a thorough search on YouTube.

com (**A4**). The findings indicated that the video ad named '*Pentru cetățenii români*' ('For the Romanian citizens') was posted on 6 May 2023 by the *România astăzi* (România Today) channel and reached over 3.65 million viewers and received 2.1K like reactions and 23 comments (figures from 22 May 2023) (**R6**). The YouTube channel ID @Romaniaastazi-zl2pj has 4.22K subscribers (on 22 May 2023, the day of capture) who joined YouTube on 4 May 2023 (**R7**). By searching for the original video on YouTube, we found that the ad was erased from the initial channel playlist, but it was running as a loop video into a low-profile user playlist. This finding has two meanings: it is a technique used for hiding a video in a shuffle playlist (**T5**) or it is a simple fingerprint generated accidentally by an inexperienced YouTube user. The video ad named 'For the Romanian citizens' was identified in the playlist of user @peisaj131 (URL: https://www.youtube.com/@peisaj131) (**R8**). In this playlist, the video keeps the initial owner names that appear to be the channel named 'Romania Today' – @romaniaastazi-zl2pj (URL: https://www.youtube.com/@romaniaastazi-zl2pj). The profile picture was the evidence of using this channel to manage the video ad campaign (**R9**). At the time of writing this paper, the @romaniaastazi-zl2pj channel was changed to @EvelynTraders – Evelyn Morgan, located in the United States, which shares many videos about FOREX trading to make money easier (**R10**). Meanwhile, the channel has reached 6.86K subscribers (URL: https://www.youtube.com/channel/UCWXYuujcE4lw_JCaLxHeU9Q).

The next purpose (**P4**) refers to finding additional information about the content of the policy page by performing a Google search. With the name 'data controller', Mihailov Ivan Sergheevici (**A5**), two other sites with the same model privacy policy page in Romania, were identified: Kishoregoldsmith.com and pineridgedevelopers.com **(R11)**. The technique identified shows the use of a fake privacy policy (**T6**), an automated translation with some Russian legal references included, without any relevance of data protection of Romanian audience/users.

To explore the website history (**P5**), we checked the Archive.org database for all the websites related to the campaign: hhx.theteachingmentors.com, gute.mycalculat.com, quoxc.moneyflowgroup.com, kishoregoldsmith.com and pineridgedevelopers.com (**A6**). All the sites appear to be compromised or captured by attackers (**R12**). They displayed error pages or bad connections during the analysis, and some of them appeared to have no records, while some of the captured pages were deleted from the tracking records. Thus, the technique identified is that of erasing public records of digital fingerprints as part of information laundering (**T7**). The next step was checking for Google indexing websites (**A7**) to determine the history of the website on the Internet. During this stage, we discovered that all websites appeared to have a history of at least 2 years and were not created only for this campaign (**R13**). This information led to the technique of using comprised or captured websites (**T8**).

The next purpose is to check for digital identity (**P6**) by searching for domain and subdomain names in multiple databases: who.is, whois.com, subdomains.whoisxmlapi.com, and criminalip.io (**A7**). According to our findings, the domain names of all identified websites had the same name servers in the same class C subnet (the first three numbers of their IPs were identical), meaning that the websites were hosted and managed from the same place (**R14**). Using the WhoisXML API subdomain search tools, it appeared that the subdomains used in this campaign were created between 19 May and 23 May 2023 (**R15**). Using who.is and whois.com, all domains shared the same name servers even if they had different registrars – 162.159.24.201/ns1.dns-parking.com/ns2.dns-parking.com (**R16**). The technique identified consists of phishers using subdomain tricks, namely redirecting to compromised sites with custom subdomains for evasion (**T9**). If attackers use different evasion techniques, then OSINT analysis should be more comprehensive by including the tactic of checking subdomain names as domain names using who.is, whois.com tools (**A8**). In this way, the technique of mixing valid domain names can be used to obtain a subdomain name (**T10**). The findings led to other compromised websites from China, Spain, Pakistan, and the UAE (**R17**). This information led to a new technique that combined many domain names as subdomains for evasion and confusion.

In the next step of tracking digital identity, we carried out cross-social platform checking on Facebook (**A9**) and found that the website theteachingmentors.com was associated with the Teaching Mentors Facebook page (**R18**). The dialling code mentioned on this page led to Pakistan (**R19**). This finding confirmed the technique of using compromised identity for legitimacy (**T11**).

Finally, we also checked for any scam or malicious disclosed activity (**P7**) by verifying all the websites in the virustotal.com, scamadviser.com and webparanoid.com databases (**A10**). The Virus Total results for quoxc.moneyflowgroup.com revealed one security vendor flagging this URL as malicious (**R20**). No other security vendors flagged these websites for malicious activity, such as scam or phishing campaigns (**T12**).

To conclude, all seven purposes of the analysis involved 10 actions that had 20 results and revealed 12 techniques used in this case of cognitive hacking that blended information operations with cyber threat capabilities.

3.5. Tagging Research with the DISARM Framework

The next step in proving a malicious campaign is to match the technological determinants of cognitive hacking with the patterns of influence operations. In this case, we labelled our technical findings under the DISARM framework using DISARM Word Plug-In. Finding attacker behaviours and identifying their tactics and techniques create a behavioural profile based on the DISARM Red Framework – incident creator TTPs, which was useful for determining kill chain attacks.

The use of anonymous and generic names on social platforms (**T1**) is associated with Create Inauthentic Social Media Pages and Groups [T0007], Identify Social and Technical Vulnerabilities: Identify Media System Vulnerabilities [T0081.008]), Create Personas [T0097], Conceal Information Assets: Use Pseudonyms [T0128.001], Conceal Information Assets: Conceal Network Identity [T0128.002], Create Inauthentic Accounts [T0090], Create Inauthentic Accounts: Create Anonymous Accounts [T0090.001], and Conceal Information Assets: Use Pseudonyms [T0128.001].

The compromise of the public newsfeed website to plant fake article on a public newsfeed that mixes the false information with the excerpts copied from an authentic news website (**T2**) is associated with the Compromise Legitimate Accounts [T0011], Compromise Legitimate Accounts [T0011], Distort Facts [T0023], Distort Facts: Edit Open-Source Content [T0023.002], Flooding the Information Space: Bots Amplify via Automated Forwarding and Reposting [T0049.003], Reuse Existing Content [T0084], Reuse Existing Content: Use Copypasta [T0084.001], and Reuse Existing Content: Plagiarize Content [T0084.002].

AI-generated voice-over for a stock video (**T3**) and the use of deepfake content (**T4**) are mentioned in Create Clickbait [T0016], Develop Image-Based Content: Develop AI-Generated Images (Deepfakes) [T0086.002], Develop Video-Based Content: Develop AI-Generated Videos (Deepfakes) [T0087.001], and Develop Audio-Based Content: Develop AI-Generated Audio (Deepfakes) [T0088.001].

The use of a translated fake privacy policy (**T6**) machine is identified in Distort Facts: Edit Open-Source Content [T0023.002], Reuse Existing

Content [T0084], Reuse Existing Content: Use Copypasta [T0084.001], Reuse Existing Content: Plagiarise Content [T0084.002], and Reuse Existing Content: Deceptively Labeled or Translated [T0084.003].

Redirecting to comprised or captured websites (**T8**) and using compromised identities for legitimacy (**T11**) are associated with compromise legacy accounts [T0011], build networks: create organisations [T0092.001], prepare assets impersonating legitimate entities [T0099], control information environments through intensive cyberspace operations: conduct server redirect [T0123.004], conventional operational activity: Redirect URLs [T0129.008], and create automatic websites [T0013].

Deleting tracking records (**T7**), customising subdomains (**T9**), mixing valid domain names to obtain a subdomain name (**T10**), or hiding a video in a shuffle playlist **(T5**) are not tagged as evasion techniques in DISARM, but these techniques are correlated with Compromise Legitimate Accounts [T0011], Harass: Threaten to Dox [T0048.003], Harass: Dox [T0048.004], Map Target Audience Information Environment [T0080], Identify Social and Technical Vulnerabilities [T0081], Infiltrate Existing Networks [T0094], and Conceal Information Assets: Launder Information Assets [T0128.004].

The malicious activity of the website identified as scam or phishing campaigns (**T12**) is associated with the Control Information Environment through Offensive Cyberspace Operations [T0123] and Make Money: Scam [T0137.002].

Summarising the TTPs uncovered by the OSINT analysis based on the PART model and tagging them under the DISARM framework, the overall picture of this cognitive hacking case revealed the intentions, persistence, and level of sophistication of the influencing actors behind this misleading campaign.

4. Discussion

The practice of using the DISARM framework for analysing the cognitive hacking case in Romania was proved to be as reliable as the analysis of the targeted misinformation, disinformation, and malinformation (MDM) campaigns driven by two specific Russian campaigns in Italy surrounding the war in Ukraine [57].

This level of analysis has limitations in terms of technical attribution. There was evidence of hostile actors, such as Russian privacy policy pages, but nothing to conclusively tie it to a specific hostile state. The use of national symbols or remarks about the state's reputation could be much more related to a FIMI operation. Without them, these misleading ads could easily be associated with common cybercrime.

At the same time, as **R10** has proven, attackers can cover their digital fingerprints by changing the name and activity of the channels used in the influence campaign, which makes their tracking more difficult. Given the absence of a clear public beneficiary for this advertising campaign, the following question arises: Who would invest funds to establish this content engine and execute the malvertising campaign? Perhaps the tech companies managing the advertising platforms could easily uncover the answer by tracking the source of funding. Instead, as researchers, you have to hope for a potential answer by tracking operational patterns over time, leveraging the identified modus operandi based on TTPs.

Another concern relates to the possible impact of these misleading advertising campaigns whose efforts to materialise do not seem to make sense at first sight. A high level of uncertainty, no obvious financial motivation, and the absence of any legally responsible entity could be the predictors of the cognitive hacking deployed for social harm or political pressure.

In the context of countering cyber-enabled FIMI, any practical approach to existing tools can improve defence strategies by updating TTPs, similar to the sharing databases used in cybersecurity. When confronted with a hybrid threat, response actions should be combined starting at the strategic level. In our research, the meta-analysis based on the strategic structured PART model could be replicated and improved by other researchers, building on other cases and with more sophisticated tools. Tagging the findings into the DISARM framework can prove their two-fold utility. On the one hand, it can confirm the effectiveness of the framework by linking it to already identified techniques; on the other hand, it can improve the framework by adding new techniques, given the constant evolution of cyber threats.

5. Conclusions

This in-depth analysis of a cognitive hacking case can provide the basis for a set of new methodologies for exposing malicious interference in people's minds. Starting from nothing more than the identification of apparently irrelevant video ads, which are usually ignored by analysts, using open tools, and accessing public databases can reveal a malicious scheme that blends information operations with cyber threat capabilities. This analysis was carried out from the perspective of two regular Internet users with an average level of digital literacy and awareness of cyber threats and no sophisticated online tools.

The research involved 10 steps, provided 20 results and revealed 12 techniques used in this case of cognitive hacking. Using AI-generated content in deepfake ads, hijacking websites and planting fabricated content under anonymity, abusing social networks, and purchasing targeted advertisements to manipulate vulnerable social groups are well-known tactics and techniques used in the preparedness stage of cyber influence operations.

The remaining question is, what to do with such cases that, at first sight, appear to have no discernible association with any specific entity or purpose or that do not overtly indicate any explicit threat. Should they be dismissed as irrelevant? Based on this in-depth analysis, when there is no clear evidence of what entity is involved and for what purpose, such situations can provide early warning of a potential attack in the preparatory stage. Detecting these signs early, before the actions as such manage to alter the analysts' perspective on what happens and how it happens, can reinforce defence mechanisms, and thwart malicious actions in their infancy, which is the most desirable scenario for defence. The extensive analysis of the identified case builds confidence that applying the DISARM framework to cyber-enabled influence campaigns can be useful for anticipating cyfluence and FIMI operations, even when such operations do not appear to have specific, immediately identifiable perpetrators or purposes.

References

[1] A.K. Sood, R.J. Enbody, "Malvertising – exploiting web advertising," *Computer Fraud & Security*, vol. 2011, no. 4, pp. 11–16, 2011, doi: 10.1016/S1361-3723(11)70041-0.

[2] C. Dwyer, A.A. Kanguri, "Malvertising – A rising threat to the online ecosystem," *Journal of Information Systems Applied Research (JISAR)*, vol. 10, p. 29, 2017.

[3] M. Willett, "The cyber dimension of the Russia–Ukraine war," *Survival (Lond)*, vol. 64, no. 5, pp. 7–26, 2022, doi: 10.1080/00396338.2022.2126193.

[4] K. Poireault. (Nov. 18, 2023). "Russian APT Sandworm disrupted power in Ukraine using novel OT techniques," *Infosecurity Magazine*. [Online]. Available: https://www.infosecurity-magazine.com/news/russia-sandworm-disrupted-power. [Accessed: Jun. 25, 2023].

[5] G. Pakharenko, "Cyber operations at Maidan: A first-hand account," in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn: NATO–CCD-COE Publications, 2015, pp. 59-66. [Online]. Available: https://ccdcoe.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf [Accessed: Jun. 25, 2023].

[6] J. Przetacznik, S. Tarpova. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. [Online]. Available: https://epthinktank.eu/2022/06/21/russias-war-on-ukraine-timeline-of-cyber-attacks. [Accessed: Jun. 25, 2023].

[7] Microsoft. (2022). *Defending Ukraine: Early lessons from the cyber war*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war. [Accessed: Apr. 11, 2023].

[8] G. Wilde. (Dec. 12, 2022). *Cyber operations in Ukraine: Russia's unmet expectations*. [Online]. Available: https://carnegieendowment.org/research/2022/12/cyber-operations-in-ukraine-russias-unmet-expectations?lang=en. [Accessed: Mar. 9, 2023].

[9] A. MacDonald, R. Ratcliffe. (Nov. 18, 2023). *Cognitive warfare: maneuvering in the human dimension*. [Online]. Available: https://www.usni.org/magazines/proceedings/2023/April/cognitive-warfare-maneuvering-human-dimension. [Accessed: Dec. 03, 2023].

[10] D. Susser, B. Roessler, H. Nissenbaum, "Online manipulation: Hidden influences in a digital world," *Georgetown Law Technology Review*, vol. 1, pp. 1–45, 2019, doi: 10.2139/ssrn.3306006.

[11] R. Medrano. (2023). *Cognitive warfare: Halting the Russian sphere of influence*. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1200752.pdf. [Accessed: Dec. 12, 2023].

[12] Y. Danyk, C.M. Briggs, "Modern cognitive operations and hybrid warfare," *Journal of Strategic Security*, vol. 16, no. 1, pp. 35–50, 2023, doi: 10.2307/48718245.

[13] P. Krawczyk, J. Wiśnicki, "Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022," *Cybersecurity and Law*, vol. 9, no. 1, pp. 194–203, 2023, doi: 10.35467/cal/169315.

[14] J.F. Tripp, N.K. Lankton, D.H. Mcknight, J. Tripp, "Technology, humanness, and trust: rethinking trust in technology," *Journal of the Association for Information Research*, vol. 16, no. 10, pp. 880–918, 2015, doi: 10.17705/1jais.00411.

[15] D.B. Hollis, "The influence of war; the war for influence," *Temple International & Comparative Law Journal*, vol. 32, no. 1, pp. 31, 2018.

[16] G. Cybenko, A. Giani, P. Thompson, "Cognitive hacking," *Advances in Computers*, vol. 60, pp. 35–73, 2004, doi: 10.1016/S0065-2458(03)60002-1.

[17] NATO Allied Command Transformation. (Nov. 18, 2023). *Cognitive warfare: Strengthening and defending the mind*. [Online]. Available: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind. [Accessed: Dec. 13, 2023].

[18] A. Ertan, K.H. Floyd, P. Pernik, T. Stevens. (2020). *Cyber threats and NATO 2030: Horizon scanning and analysis*. [Online]. Available: https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis. [Accessed: Jun. 25, 2023].

[19] O. Backes, A. Swab. (2019). *Cognitive warfare: The Russian threat to election integrity in the Baltic states*. [Online]. Available: https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states. [Accessed: Dec. 23, 2023].

[20] A. Bernal, C. Carter, I. Singh, K. Cao, O. Madreperla. (2020). *Cognitive warfare: An attack on truth and thought*. [Online]. Available: https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf. [Accessed: Nov. 18, 2023].

[21] N. Beauchamp-Mustafaga, "Cognitive domain operations: The PLA's new holistic concept for influence operations," *China Brief*, vol. 19, no. 16, 2019. [Online]. Available: https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations. [Accessed: Nov. 18, 2023].

[22] L. Hauser, *Coordinated chaos: Synchronized cyberwarfare and disinformation attacks.* The Project on International Peace and Security. Williamsburg, VA: Global Research Institute, 2022.

[23] R. Burda, *Cognitive warfare as part of society never-ending battle for minds. Information-based behavioral influencing and Western practice paper series*. The Hague: The Hague Centre for Strategic Studies, Jun 23, 2023.

[24] M. Alazab, "Russia is using an onslaught of cyber attacks to undermine Ukraine's defense capabilities," *The Conversation*, 24 Feb. 2022. [Online]. Available: https://theconversation.com/russia-is-using-an-onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638. [Accessed: Mar. 30, 2022].

[25] A. Wahlstrom, A. Revelli, S. Riddell, D. Mainor, R. Serabian. (2022). *The IO offensive: Information operations surrounding the Russian invasion of Ukraine*. [Online]. Available: https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine. [Accessed: Nov. 18, 2023].

[26] I. Yonat. (2023). *Hostile influence campaigns, cyber security and AI*. [Online]. Available: https://www.linkedin.com/posts/itai-y-5731a146_hostile-influence-campaigns-cyber-security-activity-7077365346583609344-44PL. [Accessed: Nov. 18, 2023].

[27] D. Pereira. (2023). *Cognitive infrastructure worldwide is under attack in "the worst cognitive warfare conditions since WWII."* [Online]. Available: https://www.oodaloop.com/archive/2023/11/08/cognitive-infrastructure-worldwide-is-underattack-in-the-worst-cognitive-warfare-conditions-since-wwii. [Accessed: Nov. 18, 2023].

[28] B. Gourley. (2019). *America's most critical infrastructure is also our most neglected infrastructure*. [Online]. Available: https://www.oodaloop.com/archive/2019/09/03/americas-most-critical-infrastructure-is-also-our-most-neglected-infrastructure. [Accessed: Nov. 18, 2023].

[29] Swedish Psychological Defense Agency. (2023). [Online]. Available: https://www.mpf.se/en/about-us. [Accessed: Nov. 18, 2023].

[30] Joint Research Centre EU. (2020). *Cybersecurity, our digital anchor: A European perspective*, Publications Office of the European Union, Luxembourg. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC121051. [Accessed: Nov. 18, 2023].

[31] A. Polyakova, S.P. Boyer, B.-R. Bosch. (2018). *The future of political warfare: Russia, the West, and the coming age of global digital competition*. [Online].

Available: https://www.brookings.edu/articles/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition. [Accessed Mar. 30, 2022].

[32] P.N. Petratos, "Misinformation, disinformation, and fake news: Cyber risks to business," *Business Horizons*, vol. 64, no. 6, pp. 763–774, 2021, doi: 10.1016/j.bushor.2021.07.012.

[33] US Department of State. (2020). *GEC special report: Pillars of Russia's disinformation and propaganda ecosystem*. [Online]. Available: https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report. [Accessed: Mar. 30, 2022].

[34] M. Baezner, *Cyber and information warfare in the Ukrainian conflict*. ETH Zürich: Center for Security Studies (CSS), 2018.

[35] P. Brangetto, M. A. Veenendaal. (2016). "Influence cyber operations: The use of cyberattacks in support of influence operations." 8th International Conference on Cyber Conflict, 2016, pp. 113–126. [Online]. Available: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf. [Accessed: Mar. 30, 2022].

[36] European Union Agency for Cybersecurity – ENISA. (2021). *ENISA threat landscape 2021*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. [Accessed: Mar. 30, 2022].

[37] European Commission. (Dec. 14, 2020). *The EU's cybersecurity strategy for the digital decade*. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [Accessed: Nov. 18, 2023].

[38] Y. Danyk, T. Maliarchuk, C. Briggs, "Hybrid war: High-tech, information and cyber conflicts," *Connections: The Quarterly Journal*, vol. 16, no. 2, pp. 5–24, 2017, doi: 10.11610/connections.16.2.01.

[39] D. Ardia, E. Ringel, V. S. Ekstrand, A. Fox, "Addressing the decline of local news, rise of platforms, and spread of mis-and disinformation online: A summary of current research and policy proposals," *UNC Legal Studies Research Paper,* 15 Jan. 2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3765576. [Accessed: Nov. 18, 2023].

[40] B. Martens, L. Aguiar, E. Gomez-Herrera, F. Mueller-Langer. (2018). *The digital transformation of news media and the rise of disinformation and fake news – An economic perspective*. [Online]. Available: https://ec.europa.eu/jrc. [Accessed: Nov. 18, 2023].

[41] J.T. Rob, J.N. Shapiro. (Jun. 12, 2022). *A brief history of online influence operations*. [Online]. Available: https://www.lawfareblog.com/brief-history-online-influence-operations. [Accessed: Nov. 18, 2023].

[42] P. M. Duggan, "Strategic development of special warfare in cyberspace," *Joint Force Quarterly 79*, vol. 79, no. 4, pp. 46–53, 2015.

[43] C. Whyte, A. T. Thrall, B. M. Mazanec, Eds., *Information warfare in the age of cyber conflict*. London, UK, New York, NY, USA: Routledge Taylor & Francis Group, 2021.

[44] C. Whyte, "Cyber conflict or democracy 'hacked'?" How cyber operations enhance information warfare," *Journal of Cybersecurity,* vol. 6, no. 1, 2020, pp. 1-17, doi: 10.1093/cybsec/tyaa013.

[45] R. Manwaring, J. Holloway, "Resilience to cyber-enabled foreign interference: Citizen understanding and threat perceptions," *Defense Studies*, vol. 23, no. 2, pp. 334–357, 2022, doi: 10.1080/14702436.2022.2138349.

[46] M.A. Gomez, "Cyber-enabled information warfare and influence operations," in *Information warfare in the age of cyber conflict*, C. Whyte, A.T. Thrall, B.M. Mazanec, Eds., London: Routledge Taylor & Francis, 2021, pp. 132–146.

[47] M. Wigell, "Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy," *International Affairs*, vol. 95, no. 2, pp. 255–275, 2019, doi: 10.1093/ia/iiz018.

[48] M. Weissmann, N. Nilsson, B. Palmertz, P. Thunholm, Eds., *Hybrid warfare: Security and asymmetric conflict in international relations.* London: I.B. Tauris, 2021.

[49] M.E. Zurko, "Disinformation and reflections from usable security," *IEEE Security and Privacy*, vol. 20, no. 3., pp. 4–7, 2022, doi: 10.1109/MSEC.2022.3159405.

[50] I. Lella, M. Theocharidou, E. Tsekmezoglou, R. Svetozarov Naydenov, C. Ciobanu, A. Malatras. (2022). *ENISA threat landscape 2022*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed: Aug. 20, 2023].

[51] C. R. Walker, S.-J. Terp, P. C. Breuer, C. L. Crooks, "Misinfosec," Companion Proceedings of The 2019 World Wide Web Conference. Association for Computing Machinery, May 13, pp. 1026–1032, 2019. doi: 10.1145/3308560.3316742.

[52] DISARM Foundation. (Nov. 12, 2023). *DISARM framework*. [Online]. Available: https://www.disarm.foundation/framework. [Accessed: Nov. 18, 2023].

[53] EU-US Trade and Technology Council. (May 31, 2023). *Trade and Technology Council Fourth Ministerial – Annex on foreign information manipulation and interference in third countries*. [Online]. Available: https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en. [Accessed: Mar. 22, 2024].

[54] S. Terp, P. Breuer. (2022). "DISARM: A framework for analysis of disinformation campaigns." 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), Salerno, Italy, pp. 1–8, doi: 10.1109/CogSIMA54611.2022.9830669.

[55] H. Newman. (2022). *Foreign information manipulation and interference defense standards: Test for rapid adoption of the common language and framework "DISARM."* [Online]. Available: https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253. [Accessed: Mar. 30, 2022].

[56] R. Arcos. (2018). *Post event analysis of the hybrid threat security environment: assessment of influence communication operations.* [Online]. Available: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-12-postevent-analysis-of-the-hybrid-threat-security-environment-assessment-of-influence-communication-operations. [Accessed: Nov. 12, 2023].

[57] M. Lesser, H.J. Stern, S.J. Terp. (2022). "Countering Russian misinformation, disinformation, malinformation and influence campaigns in Italy surrounding the Russian invasion of Ukraine," *International Forum on Digital and Democracy 2022*. [Online]. Available: https://ceur-ws.org/Vol-3289/paper2.pdf. [Accessed: Nov. 12, 2023].

ANNEX 1. Screenshots of the case identification stage

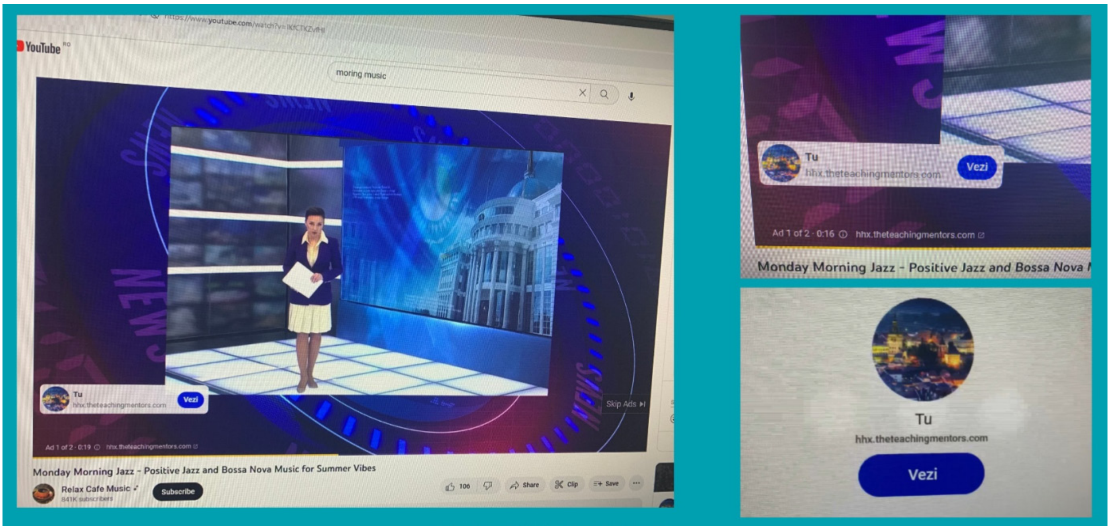

YouTube
moring music
Tu
hhx.theteachingmentors.com
Vezi
Skip Ads
Ad 1 of 2 · 0:19 · hhx.theteachingmentors.com
Monday Morning Jazz - Positive Jazz and Bossa Nova Music for Summer Vibes
Relax Cafe Music
Subscribe
106
Share
Clip
Save
Ad 1 of 2 · 0:16 · hhx.theteachingmentors.com
Monday Morning Jazz - Positive Jazz and Bossa Nova

Photo captured from the first video ad promoted on YouTube.

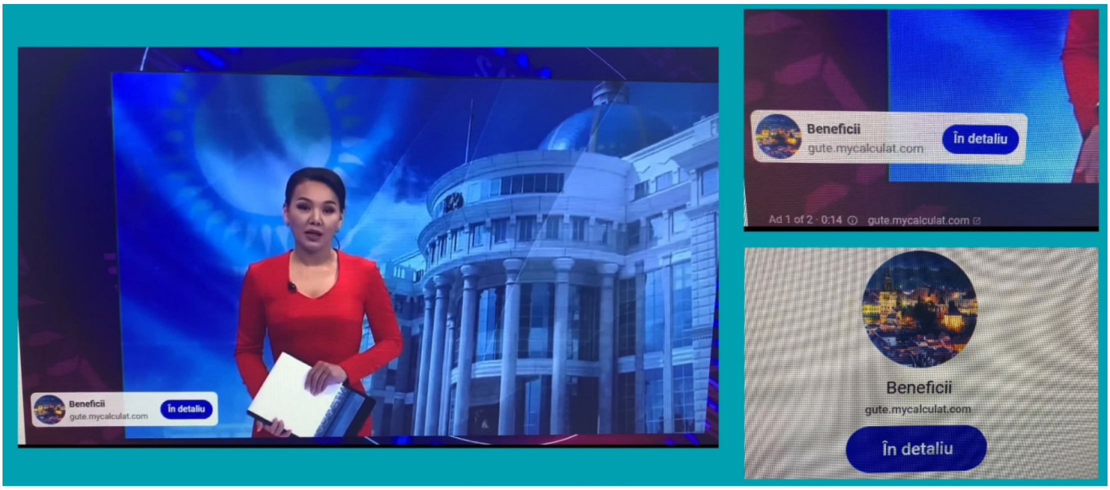
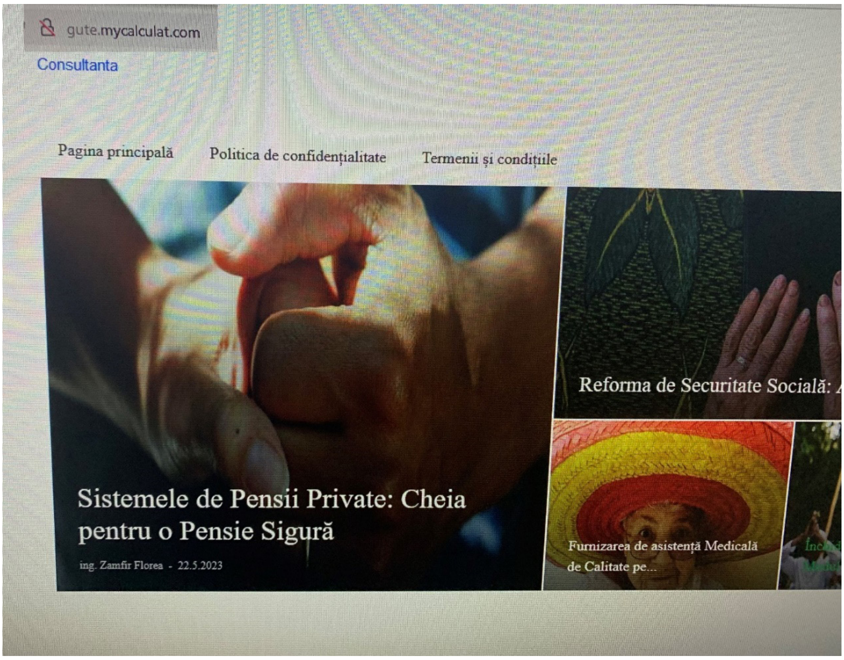
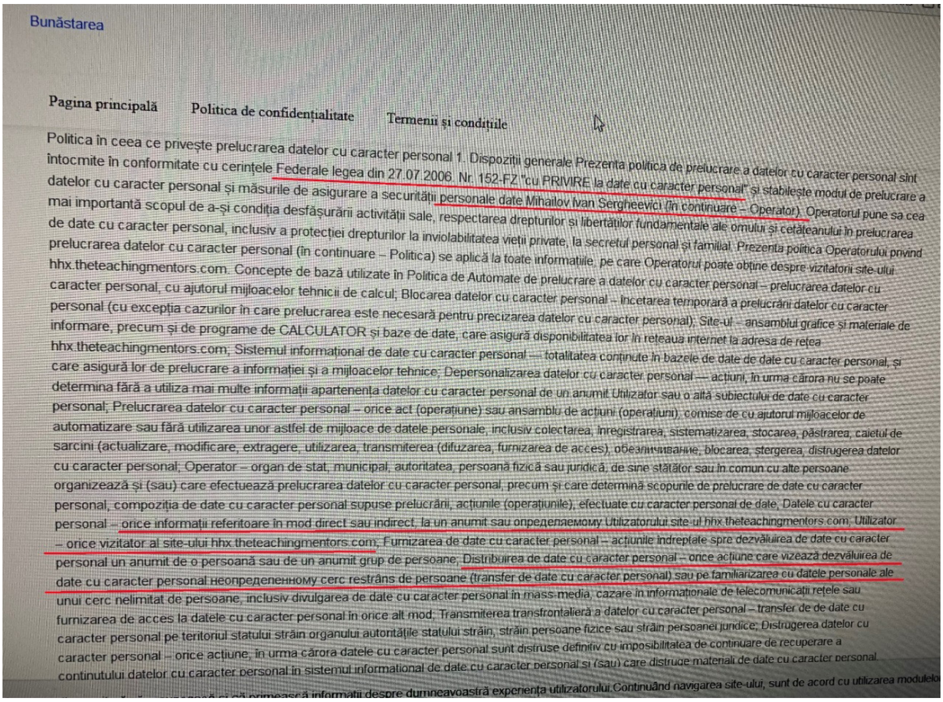


Photo captured from the second video ad promoted on YouTube.

ANNEX 2. Screenshots of digital analysis


gute.mycalculat.com
Consultanta
Pagina principală
Politica de confidențialitate
Termenii și condițiile
Sistemele de Pensii Private: Cheia pentru o Pensie Sigură
ing. Zamfir Florea - 22.5.2023
Reforma de Securitate Socială: A
Furnizarea de asistență Medicală de Calitate pe...

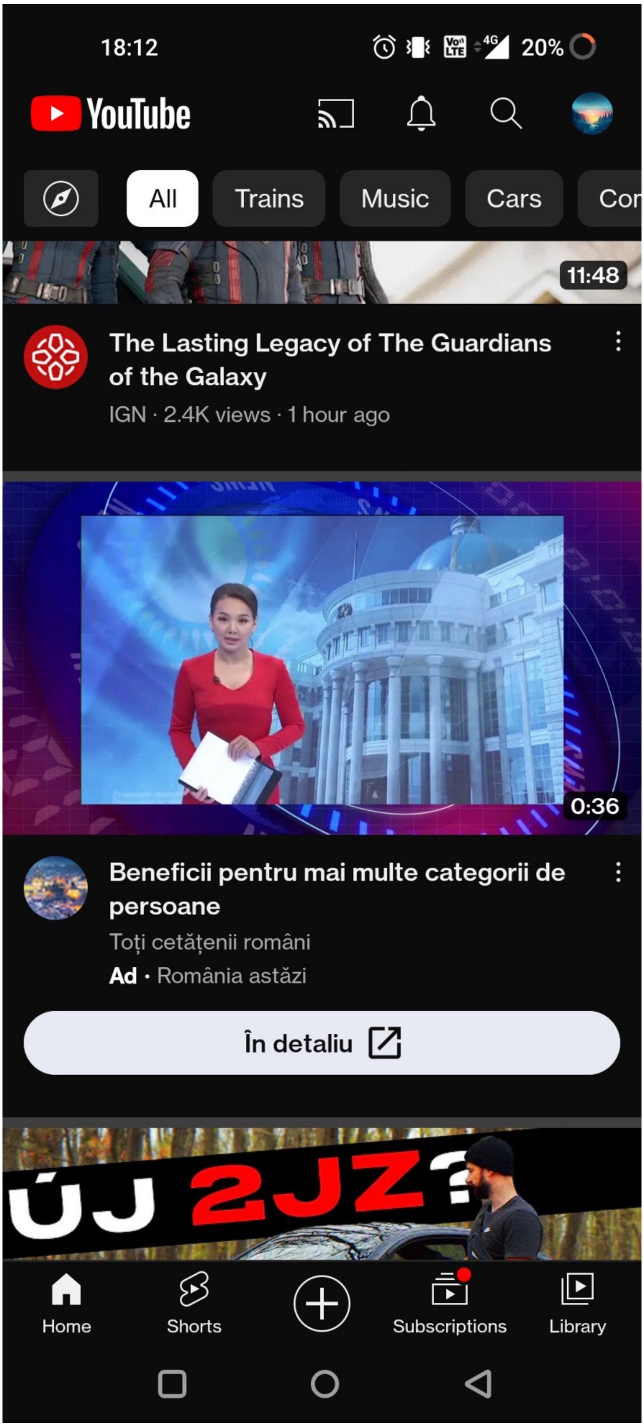
Screenshot of the website gute.mycalculat.com



Politica în ceea ce privește prelucrarea datelor cu caracter personal 1. Dispoziții generale Prezenta politica de prelucrare a datelor cu caracter personal sînt
întocmite în conformitate cu cerințele Federale legea din 27.07.2006. Nr. 152-FZ "cu PRIVIRE la date cu caracter personal" și stabilește modul de prelucrare a
datelor cu caracter personal și măsurile de asigurare a securității personale date Mihailov Ivan Sergheevici (în continuare – Operator). Operatorul pune sa cea
mai importantă scopul de a-și condiția desfășurării activității sale, respectarea drepturilor și libertăților fundamentale ale omului și cetățeanului în prelucrarea
de date cu caracter personal, inclusiv a protecției drepturilor la inviolabilitatea vieții private, la secretul personal și familial. Prezenta politica Operatorului privind
prelucrarea datelor cu caracter personal (în continuare – Politica) se aplică la toate informațiile, pe care Operatorul poate obține despre vizitatorii site-ului
hhx.theteachingmentors.com. Concepte de bază utilizate în Politica de Automate de prelucrare a datelor cu caracter personal – prelucrarea datelor cu
caracter personal, cu ajutorul mijloacelor tehnicii de calcul; Blocarea datelor cu caracter personal – încetarea temporară a prelucrării datelor cu caracter
personal (cu excepția cazurilor în care prelucrarea este necesară pentru precizarea datelor cu caracter personal); Site-ul – ansamblul grafice și materiale de
informare, precum și de programe de CALCULATOR și baze de date, care asigură disponibilitatea lor în rețeaua internet la adresa de rețea
hhx.theteachingmentors.com; Sistemul informațional de date cu caracter personal — totalitatea conținute în bazele de date de date cu caracter personal, și
care asigură lor de prelucrare a informației și a mijloacelor tehnice; Depersonalizarea datelor cu caracter personal — acțiuni, în urma cărora nu se poate
determina fără a utiliza mai multe informații apartenența datelor cu caracter personal de un anumit Utilizator sau o altă subiectului de date cu caracter
personal; Prelucrarea datelor cu caracter personal – orice act (operațiune) sau ansamblu de acțiuni (operațiuni), comise de cu ajutorul mijloacelor de
automatizare sau fără utilizarea unor astfel de mijloace de datele personale, inclusiv colectarea, înregistrarea, sistematizarea, stocarea, păstrarea, caietul de
sarcini (actualizare, modificare, extragere, utilizarea, transmiterea (difuzarea, furnizarea de acces), обезличивание, blocarea, ștergerea, distrugerea datelor
cu caracter personal; Operator – organ de stat, municipal, autoritatea, persoană fizică sau juridică, de sine stătător sau în comun cu alte persoane
organizează și (sau) care efectuează prelucrarea datelor cu caracter personal, precum și care determină scopurile de prelucrare de date cu caracter
personal, compoziția de date cu caracter personal supuse prelucrării, acțiunile (operațiunile), efectuate cu caracter personal de date; Datele cu caracter
personal – orice informații referitoare în mod direct sau indirect, la un anumit sau определяемому Utilizatorului site-ul hhx.theteachingmentors.com; Utilizator
– orice vizitator al site-ului hhx.theteachingmentors.com; Furnizarea de date cu caracter personal – acțiunile îndreptate spre dezvăluirea de date cu caracter
personal un anumit de o persoană sau de un anumit grup de persoane; Distribuirea de date cu caracter personal – orice acțiune care vizează dezvăluirea de
date cu caracter personal неопределенному cerc restrâns de persoane (transfer de date cu caracter personal) sau pe familiarizarea cu datele personale ale
unui cerc nelimitat de persoane, inclusiv divulgarea de date cu caracter personal în mass-media, cazare în informaționale de telecomunicații rețele sau
furnizarea de acces la datele cu caracter personal în orice alt mod; Transmiterea transfrontalieră a datelor cu caracter personal – transfer de de date cu
caracter personal pe teritoriul statului străin organului autoritățile statului străin, străin persoane fizice sau străin persoanei juridice; Distrugerea datelor cu
caracter personal – orice acțiune, în urma cărora datele cu caracter personal sunt distruse definitiv cu imposibilitatea de continuare de recuperare a
continutului datelor cu caracter personal in sistemul informational de date cu caracter personal si (sau) care distruge materiali de date cu caracter personal.
să primească informații despre dumneavoastră experiența utilizatorului.Continuând navigarea site-ului, sunt de acord cu utilizarea modulelo

Capture of the fake policy.

ANNEX 3. Screenshots of OSINT results



18:12 20%

The Lasting Legacy of The Guardians of the Galaxy

IGN · 2.4K views · 1 hour ago

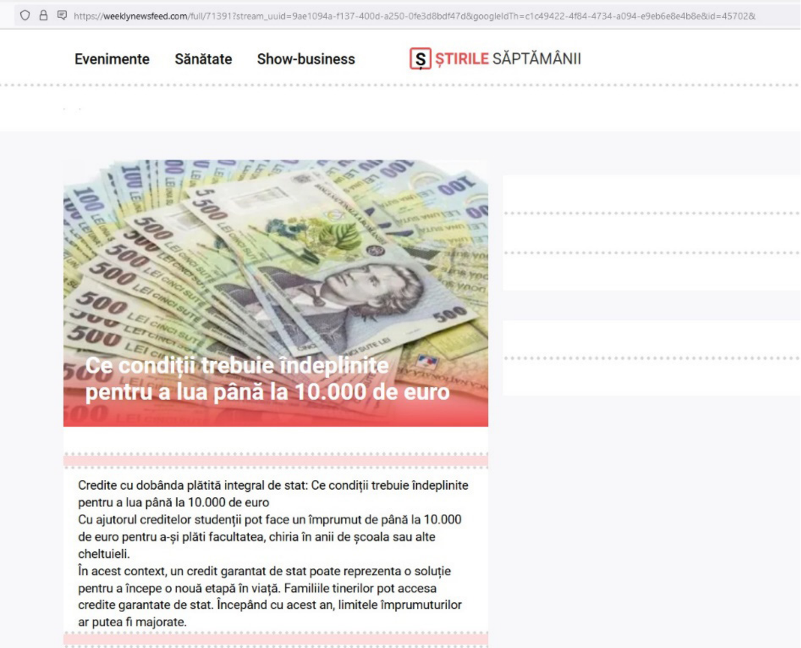
Beneficii pentru mai multe categorii de persoane

Toți cetățenii români

Ad · România astăzi

În detaliu

R1: The screenshot posted by a Reddit user who uncovered the original YouTube channel managing the video ad campaign.

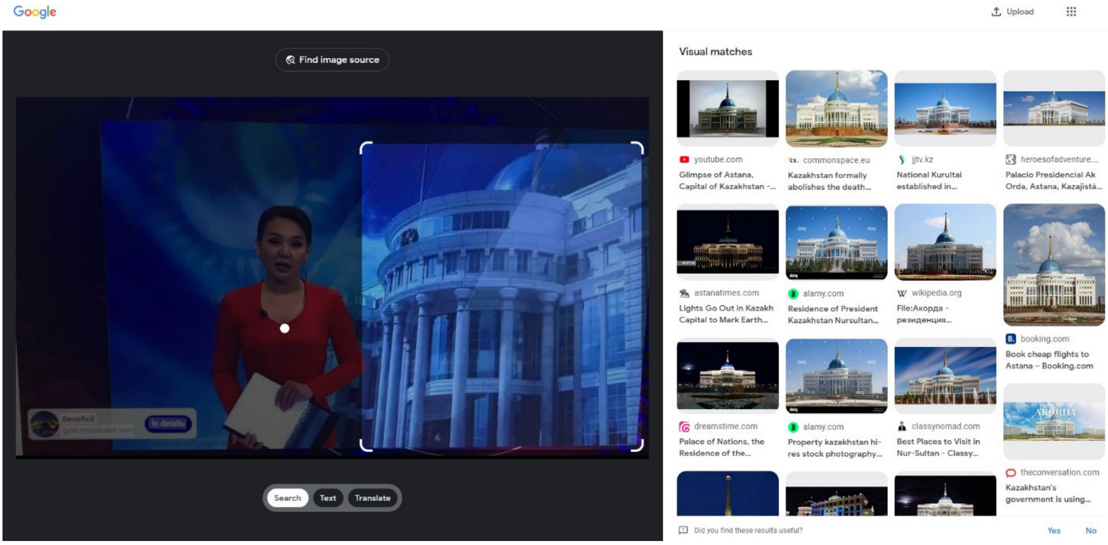


https://weeklynewsfeed.com/full/71391?stream_uuid=9ae1094a-f137-400d-a250-0fe3d8bdf47d&googleIdTh=c1c49422-4f84-4734-a094-e9eb6e8e4b8e&id=45702&

Evenimente
Sănătate
Show-business
Ș ȘTIRILE SĂPTĂMÂNII
Ce condiții trebuie îndeplinite pentru a lua până la 10.000 de euro

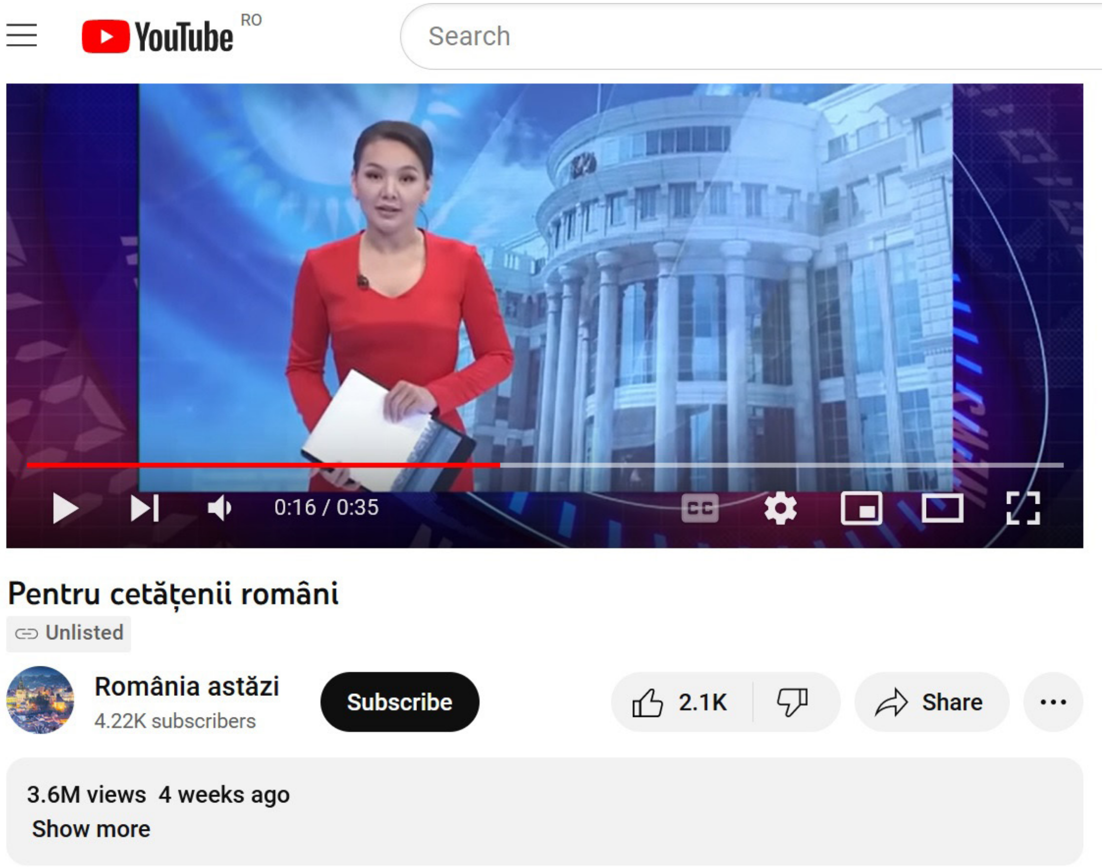
Credite cu dobânda plătită integral de stat: Ce condiții trebuie îndeplinite pentru a lua până la 10.000 de euro
Cu ajutorul creditelor studenții pot face un împrumut de până la 10.000 de euro pentru a-și plăti facultatea, chiria în anii de școala sau alte cheltuieli.
În acest context, un credit garantat de stat poate reprezenta o soluție pentru a începe o nouă etapă în viață. Familiile tinerilor pot accesa credite garantate de stat. Începând cu acest an, limitele împrumuturilor ar putea fi majorate.

R2: The fake article planted on weeklynewsfeed.com revealed by another Reddit user.



Google
Upload
Find image source
Search
Text
Translate
Visual matches
youtube.com
Glimpse of Astana, Capital of Kazakhstan -...
commonspace.eu
Kazakhstan formally abolishes the death...
jjtv.kz
National Kurultai established in...
heroesofadventure...
Palacio Presidencial Ak Orda, Astana, Kazajistá...
astanatimes.com
Lights Go Out in Kazakh Capital to Mark Earth...
alamy.com
Residence of President Kazakhstan Nursultan...
wikipedia.org
File:Акорда - резиденция...
booking.com
Book cheap flights to Astana – Booking.com
dreamstime.com
Palace of Nations, the Residence of the...
alamy.com
Property kazakhstan hi-res stock photography...
classynomad.com
Best Places to Visit in Nur-Sultan - Classy...
theconversation.com
Kazakhstan's government is using...
Did you find these results useful?
Yes
No

R4: Google images match the image footage with the Ak Orda Presidential Palace in Kazakhstan.



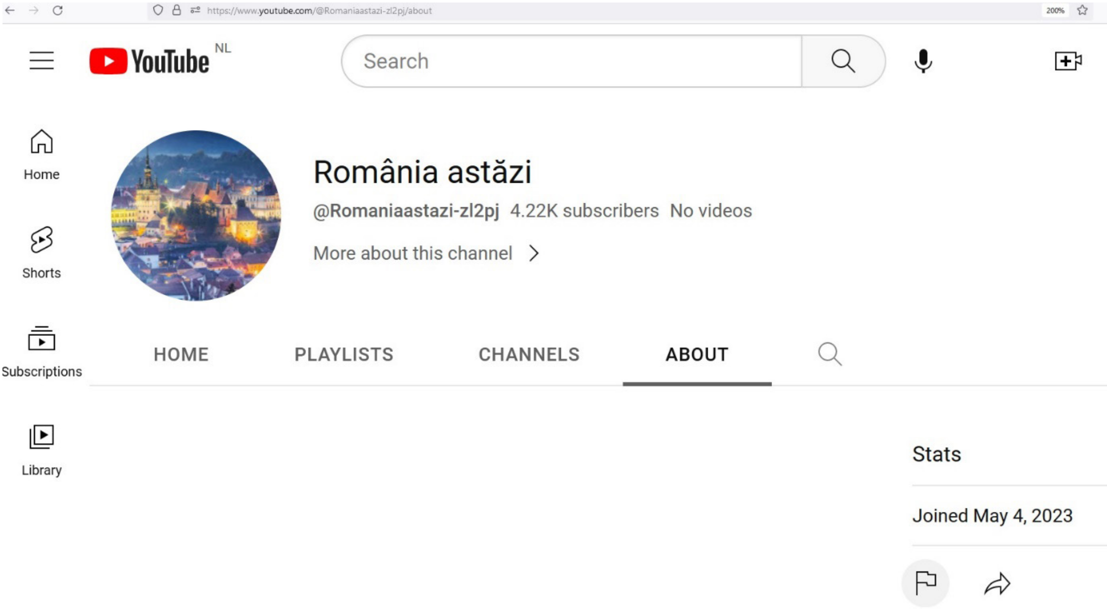
Pentru cetățenii români

Unlisted

România astăzi
4.22K subscribers

3.6M views 4 weeks ago
Show more

R6: The video ad named '*Pentru cetățenii români*' ('For Romanian Citizens') was posted on 6 May 2023 by the *România astăzi* (România Today) channel and reached over 3.65 million viewers and received 2.1K like reactions and 23 comments in 1 month (figures as on 22 May 2023).



România astăzi

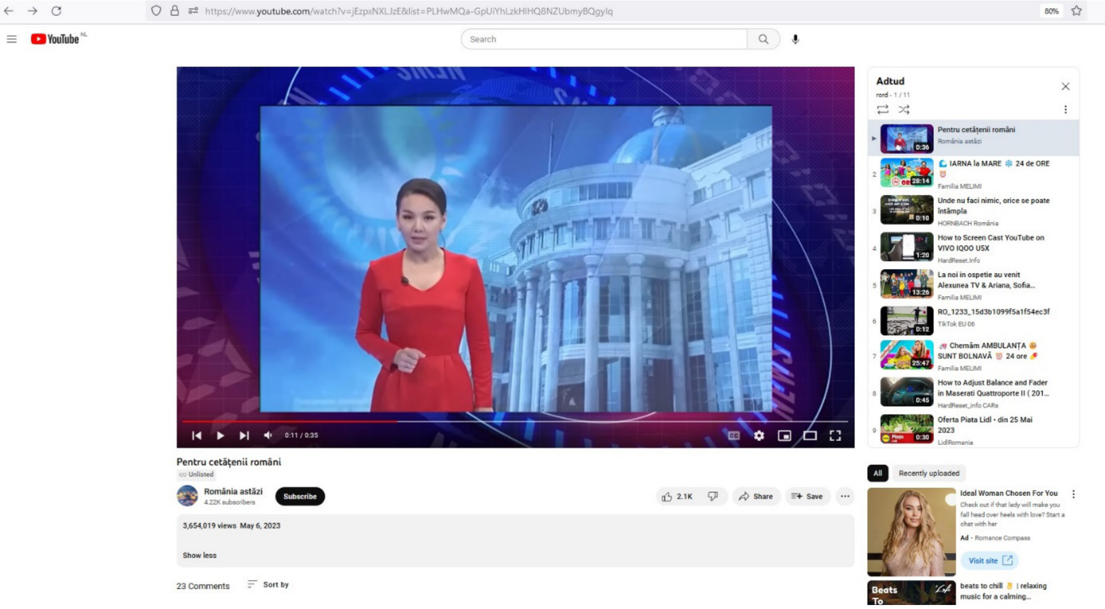
@Romaniaastazi-zl2pj 4.22K subscribers No videos

More about this channel

Stats

Joined May 4, 2023

R7: The YouTube channel ID @Romaniaastazi-zl2pj has 4.22K subscribers, joining YouTube on 4 May 2023.



Pentru cetățenii români
Unlisted

România astăzi
4.22K subscribers

3,654,019 views May 6, 2023

23 Comments

Adtud
rord - 1 / 11

Pentru cetățenii români
România astăzi
0:36

2 IARNA la MARE ❄ 24 de ORE ⏰
Familia MELIMI
28:14

3 Unde nu faci nimic, orice se poate întâmpla
HORNBACH România
0:10

4 How to Screen Cast YouTube on VIVO IQOO U5X
HardReset.Info
1:20

5 La noi in ospetie au venit Alexunea TV & Ariana, Sofia...
Familia MELIMI
13:26

6 RO_1233_15d3b1099f5a1f54ec3f
TikTok EU 06
0:12

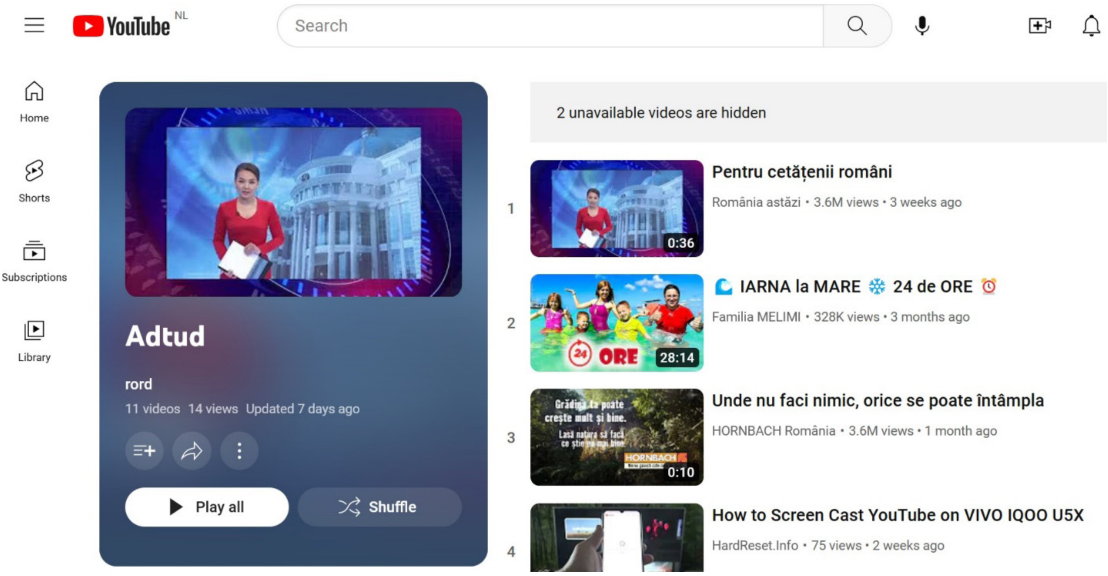
7 Chemăm AMBULANȚA SUNT BOLNAVĂ ⏰ 24 ore
Familia MELIMI
25:47

8 How to Adjust Balance and Fader in Maserati Quattroporte II (201...
HardReset_info CARs
0:45

9 Oferta Piata Lidl • din 25 Mai 2023
LidlRomania
0:30

Ideal Woman Chosen For You
Check out if that lady will make you fall head over heels with love? Start a chat with her
Ad · Romance Compass

beats to chill | relaxing music for a calming...



Adtud

rord

11 videos 14 views Updated 7 days ago

2 unavailable videos are hidden

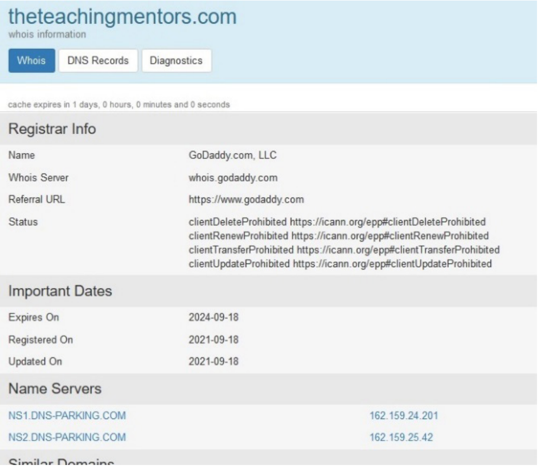
1 Pentru cetățenii români
România astăzi • 3.6M views • 3 weeks ago

2 IARNA la MARE ❄ 24 de ORE ⏰
Familia MELIMI • 328K views • 3 months ago

3 Unde nu faci nimic, orice se poate întâmpla
HORNBACH România • 3.6M views • 1 month ago

4 How to Screen Cast YouTube on VIVO IQOO U5X
HardReset.Info • 75 views • 2 weeks ago

R8: The video ad named 'For Romanian Citizens' identified in the playlist Adtud of the user *rord* aka @peisaj131 – https://www.youtube.com/@peisaj131

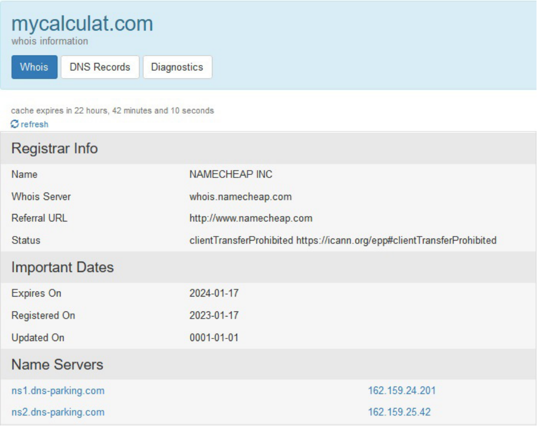


theteachingmentors.com
whois information

cache expires in 1 days, 0 hours, 0 minutes and 0 seconds

Registrar Info	
Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Important Dates	
Expires On	2024-09-18
Registered On	2021-09-18
Updated On	2021-09-18
Name Servers	
NS1.DNS-PARKING.COM	162.159.24.201
NS2.DNS-PARKING.COM	162.159.25.42

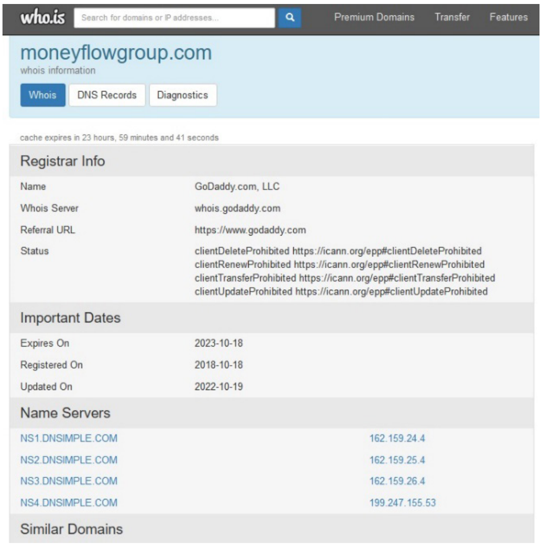
Similar Domains



mycalculat.com
whois information

cache expires in 22 hours, 42 minutes and 10 seconds

Registrar Info	
Name	NAMECHEAP INC
Whois Server	whois.namecheap.com
Referral URL	http://www.namecheap.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Important Dates	
Expires On	2024-01-17
Registered On	2023-01-17
Updated On	0001-01-01
Name Servers	
ns1.dns-parking.com	162.159.24.201
ns2.dns-parking.com	162.159.25.42



moneyflowgroup.com
whois information

cache expires in 23 hours, 59 minutes and 41 seconds

Registrar Info

Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

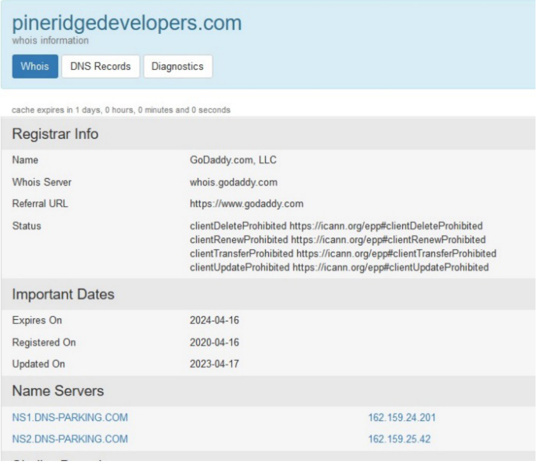
Important Dates

Expires On	2023-10-18
Registered On	2018-10-18
Updated On	2022-10-19

Name Servers

NS1.DNSIMPLE.COM	162.159.24.4
NS2.DNSIMPLE.COM	162.159.25.4
NS3.DNSIMPLE.COM	162.159.26.4
NS4.DNSIMPLE.COM	199.247.155.53

Similar Domains



pineridgedevelopers.com
whois information

cache expires in 1 days, 0 hours, 0 minutes and 0 seconds

Registrar Info

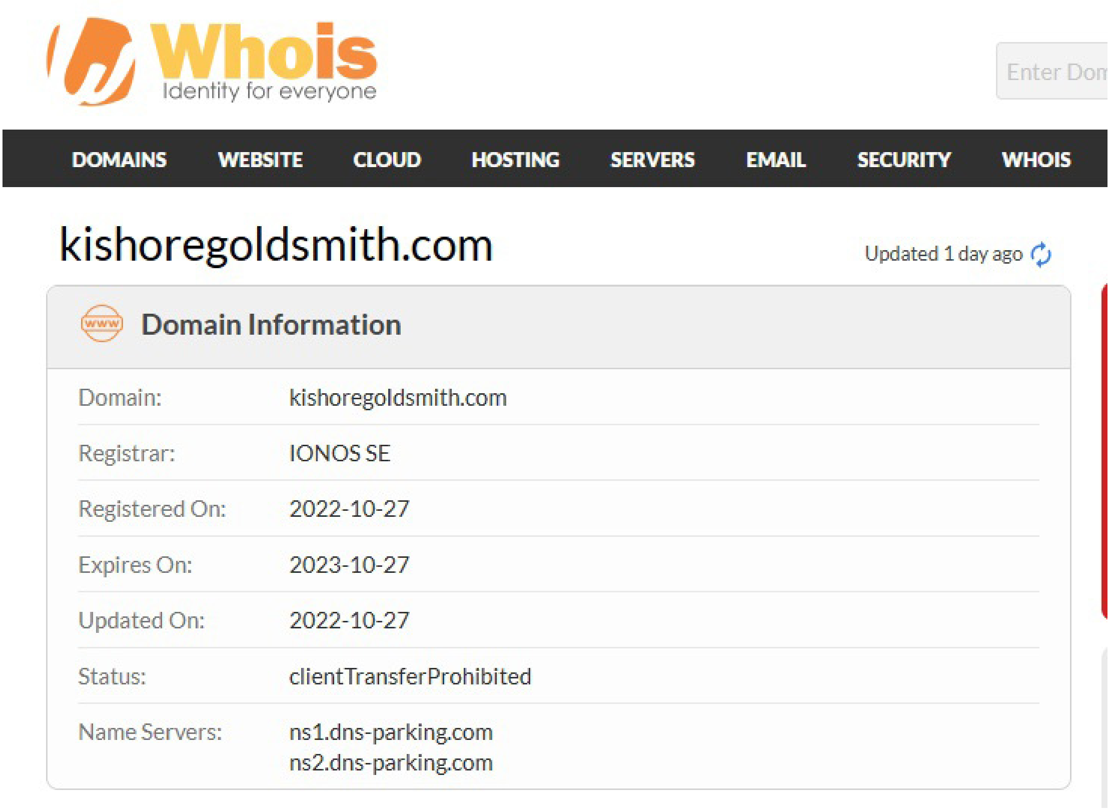
Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	2024-04-16
Registered On	2020-04-16
Updated On	2023-04-17

Name Servers

NS1.DNS-PARKING.COM	162.159.24.201
NS2.DNS-PARKING.COM	162.159.25.42



kishoregoldsmith.com

Domain Information

Domain:	kishoregoldsmith.com
Registrar:	IONOS SE
Registered On:	2022-10-27
Expires On:	2023-10-27
Updated On:	2022-10-27
Status:	clientTransferProhibited
Name Servers:	ns1.dns-parking.com ns2.dns-parking.com

R14: All identified websites have the same name servers in the same class C subnet (the first three numbers of their IPs are identical). **R16:** All domains share the same name servers even if they have different registrars – 162.159.24.201/ns1.dns-parking.com/ns2.dns-parking.com

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Military Situation Awareness: Ukrainian Experience

Viktor Putrenko | EPAM School of Digital Technology, American University Kyiv, Ukraine | ORCID: 0000-0002-0239-9241

Nataliia Pashynska | Taras Shevchenko Kyiv National University, Ukraine | ORCID: 0000-0002-0133-688X

Received: 23.11.2023

Accepted: 20.04.2024

Published: 17.07.2024

Cite this article as:
V. Putrenko,
N. Pashynska "Military situation awareness: Ukrainian experience," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190341

Corresponding author:
Viktor Putrenko, EPAM School of Digital Technology, American University Kyiv, Ukraine.
E-Mail: putrenko10@gmail.com;
00000-0002-0239-9241

Abstract

Situational awareness (SA) has become one of the key concepts in military sector. The Russian-Ukrainian war led to the development of information technology in Ukraine to manage troops and combat situations. The army was supported by numerous volunteer initiatives involving IT professionals. As a result, Ukrainian army has received modern software solutions based on the principles of SA for use in real combat conditions. The purpose of the study is to analyse the development of military and civilian SA information systems during the war between Russia and Ukraine. In the course of the study, the methods of system analysis of the problem of SA were used. The research classifies information solutions, assesses the distribution of products by different classification sectors, and conducts a strengths, weaknesses, opportunities, and threats (SWOT) analysis of the developed products. Using the example of the most common solutions, the main features of existing software products and the technologies on which they operate were identified. Prospects for the development of solutions, their contribution to military management, and problematic issues are identified.

Keywords

situational awareness, network-centric warfare, information technology, Ukraine

1. Introduction

One of the results of the war between Russia and Ukraine was the rapid growth of information technology in Ukrainian army. The main reason of this process is the need to gain an advantage over the enemy on the battlefield and in planning relevant operations. In addition to purely military components, it also includes security aspects of the management of territorial bodies that carry out regional and local governance, informing the population about the existing military and other types of hazards.

In this regard, it becomes relevant to study the formation of the most common approaches to the organisation of information interaction at the military and civilian levels based on the approaches of situational awareness (SA) and the concept of network-centric warfare (NCW). Since 2014, Ukraine has been actively developing technologies related to the information and telecommunications complex, the creation of unmanned systems, and the development of situation centres for the needs of the military sector. The joint use of the latest and updated types of weapons and these technologies allows the military to perform tasks at a new level of efficiency. Analysing this experience is important in terms of developing new approaches to military management and the use of information technology.

The goal of the study is to analyse the development of military and civilian situational awareness information systems (SAIS) during the war between Russia and Ukraine.

The objectives of the study are to analyse current trends in the development of the concept of SA, peculiarities of the use of SA tools during the war between Russia and Ukraine, trends and results of the development of information tools for SA in Ukraine, and to assess further prospects for the development of SA systems in modern wars.

In the course of the study, the methods of system analysis of SA problem based on the classification and typification of software development for military purposes were used. A conceptual modelling of the structure of the SA information system development on the basis of structural and graphical models was carried out. Separately, a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the prospects for the development of the SA information system in Ukraine was carried out. Based on the results of the analysis, perspective and problematic areas in the development of systems were identified. The characteristics of the existing developments are built and they are divided depending on the scope of military tasks and development prospects on the basis of a comparative analysis.

2. Theoretical Aspect of Situational Awareness

Situational awareness is a model of situational judgement. One of the most famous researchers in this field is Mika Endsley [1], who formed the following definition: 'SA is the perception of elements and events of the environment in relation to time or space, understanding their meaning and projecting their status in the near future'.

The purpose of SA is to actively detect and analyse information relevant to immediate operational stability and safety and to coordinate such information across the organisation to ensure that all organisational units are operating within a common operating view.

Situational awareness enables the operator to understand the operating environment of critical services and the environment that affects their performance. This understanding provides stakeholders with a reasonably accurate and relevant understanding of the past, current, and foreseeable future state of such services and supports effective decision-making in the context of the overall operating environment.

Situational awareness process establishes a common operating picture by collecting, fusing, and analysing data to support automated or human decision-making when responding to incidents. Such data must necessarily be communicated in a timely manner and in a form that allows a human to understand quickly the key elements needed to make right decisions.

The overall operational picture needs to be accurate and actionable (suitable for decision support and action). However, different participants in the process need different and not necessarily complete knowledge of the operational environment. Depending on how it is presented, a complete picture may contain too much information and overwhelm the decision-maker. Operators should also not be provided with a big amount of data. Rather, operators should only see what is important, as determined by the risk strategy and the overall risk pattern.

We present the model for SA and associated decision-making. Figure 1 depicts SA and dynamic decision-making model that

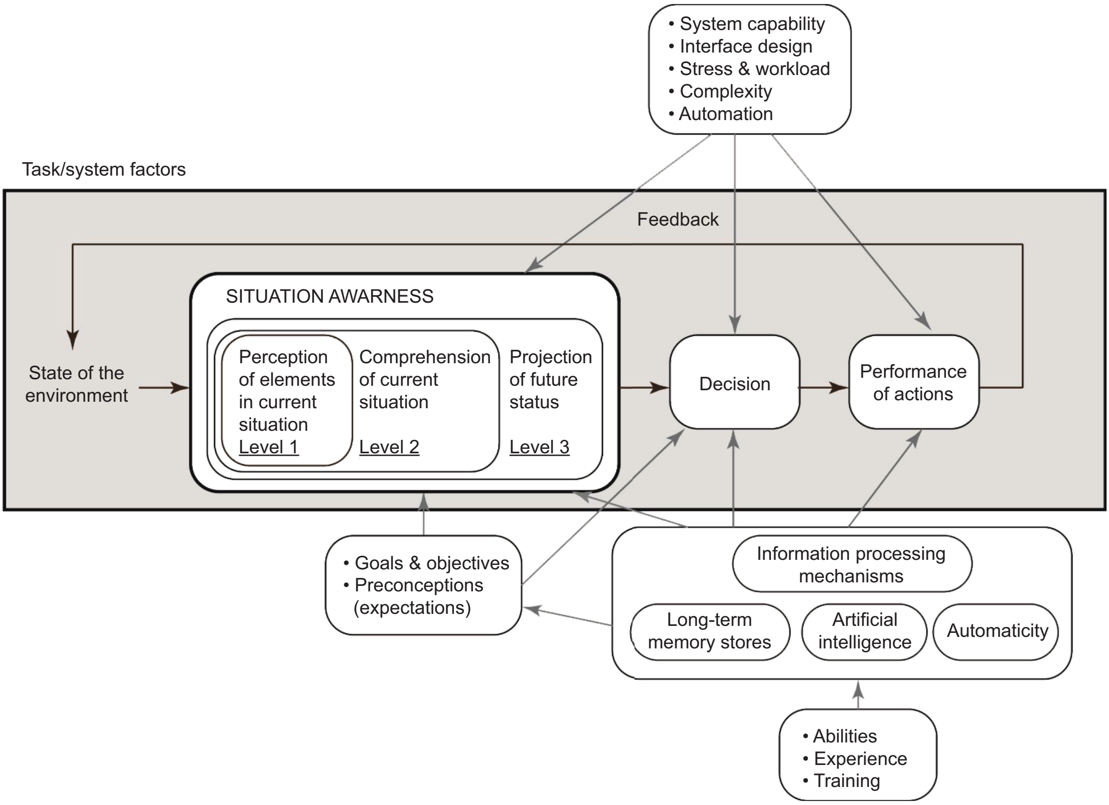


Figure 1. Modified Endsley's model of situation awareness.

has been inspired from Endsley's model of SA [1], which has been widely adopted. The model has an SA core whereas sensing and decision-making elements are built around the SA core. A multitude of sensors sense the environment to acquire the state of the environment. The sensed information is fused together to remove the redundancies in the sensed data, such as multiple similar views captured by different cameras or quantities sensed by different sensors in close locality, and also to overcome the shortcomings of the data acquired from a single source, such as occlusions, change in ambient lighting conditions, and/or chaotic elements in the environment. The fused data is then passed to the SA core, which comprises three levels or stages [2, 3].

Perception – Level 1 SA: The first stage of attaining SA is the perception of the status, attributes, and dynamics of the entities in the surroundings. For instance, an operator needs to discern important entities in the environment, such as other aircraft, terrain, and warning lights along with their pertinent characteristics [4].

Comprehension – Level 2 SA: The second stage of SA is the comprehension of the situation, which is based on the integration of disconnected level 1 SA elements. The level 2 SA is a step further than just being aware of elements in the environment as it deals with developing an understanding of the significance of those elements in relation to an operator's objectives. Concisely, we can state the level 2 of SA as understanding of entities in the surroundings, in particular when integrated together, in connection to the operator's objectives. For instance, an operator must understand the significance of the perceived elements in relation to each other. An amateur operator may be able to attain the same level 1 SA as more experienced ones, but may flounder to assimilate the perceived elements along with relevant goals to comprehend the situation fully (level 2 SA) [5].

Projection – Level 3 SA: The third level of SA relates to the ability to project the future actions of entities in the environment at least in the near term. This projection is achieved based on the cognisance of status and dynamics of elements in the environment and comprehension of the situation. Succinctly, we can state level 3 of SA as prediction or estimation of the status of entities in the surroundings in the future, at least in the near future. For example, from the perceived and comprehended information, the experienced operators predict possible future events (level 3 SA), which provides them knowledge and time to determine the most befitting course of action to achieve their objectives [6, 7].

As shown in Figure 2, the SA core also receives input from the commanders at strategic or operational levels regarding goals or objectives of SA. Our model enhances the SA model from Endsley [8] for perception, comprehension, and projection by adding support for artificial intelligence (AI)-assisted decision-making and resource management. Perception is addressed through the standard information fusion and resource management loop.

Owing to the recent advancements in AI, it has become an integral part of SA core and dynamic decision-making. AI assists operators in comprehending the situation (level 2 SA) and then making projections about the future actions of entities in the environment (level 3 SA). Thus, both robustness of AI models and operators' ability, experience, and training determine the level of comprehension acquired by the operators and the accuracy of future projections. Based on the acquired comprehension and projection, decisions are recommended by AI models to the commanders and then the commanders make appropriate decisions taking into account the

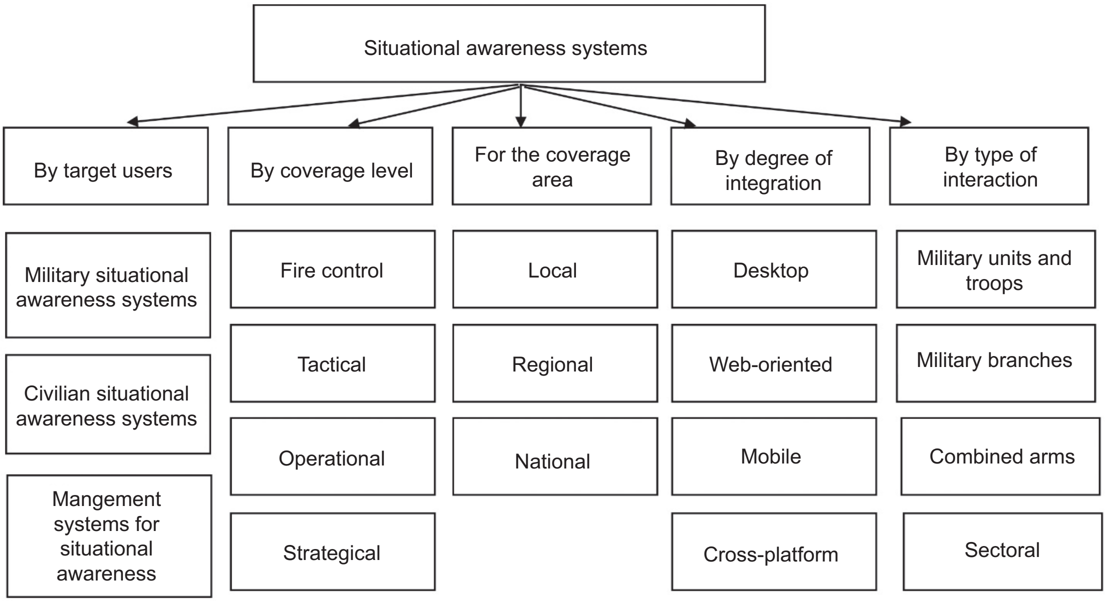


Figure 2. SAIS classification.

input from AI and the assessed situation. Finally, the decisions are implemented at tactical level by operators. The decisions to be implemented have a vast range, including, for example, the positioning of personnel and equipment, firing of weapons, medical evacuation, and logistics support [9, 10].

Situational awareness (and the operational situation as its component) are functions of time and can be represented as follows:

$$CO(t) \leq OO(t), M >,$$

CO(t) – situational awareness for a period of time *t*;

OO(t) – operational situation for a period of time *t*;

M – mental model.

The concept of ‘situational awareness’ in the context of military component analysis is very closely related to the concept of NCW [9].

The definition of NCW can be found in [11]:

> NCW is about human and organisational behaviour. At the heart of the concept of NCW is the adoption of a new

> way of thinking, network-centric and its application in military operations. The NCW concept focuses on the combat power that can be gained as a result of the network integration of military formations engaged in combat operations or the organisation of effective communication between them [12]. It is characterised by the ability of geographically dispersed forces (consisting of individual units) to create a high level of common battle space awareness that can be used through self-synchronisation and other network-centric operations to achieve the command's intent.

The definition of NCW is further elaborated on by the key concepts given in the same paper [13, 14]: 'The use of a geographically dispersed force; a high degree of awareness between the units involved in the warfare; effective communication'. Additional information about the content of the concept is provided by the basic principles of NCW (basic tenets), formulated in [15, 16]:

1. Reliable networking improves information exchange.
2. Information sharing and cooperation improve information quality and SA.
3. General SA allows for self-synchronisation.
4. Increasing the effectiveness of the mission.

3. Analysis of Ukrainian Situational Awareness Information Systems

3.1. Approaches to Classification of Situational Awareness System

The basis for analysing SAIS is a basic classification of the existing solutions in Ukraine and its comparison with international practice.

Situational awareness information systems can be classified by target users, level and geographical scope of coverage, degree of integration with information and communication platforms, and type of interaction based on them (Figure 2).

According to the general concept of military operations management and approaches to SAIS, there are four levels of information interaction at the appropriate level of coverage, which correspond to the respective classes of software and communication systems. These levels include the level of fire control on the battlefield, tactical, operational, and strategic (intelligence) levels (Figure 3). These levels are characterised by different spatial and temporal resolution

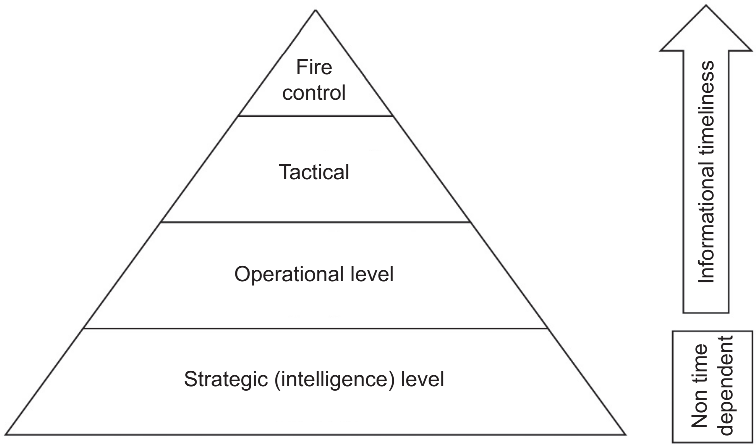


Figure 3. Levels of military control based on SAIS.

of data and the ways and methods of processing them. The speed of response to events is rapidly increasing at the fire control level, and the greatest coverage of information is important at strategic level [17].

Depending on use at different levels of combat management, the existing software solutions in the field of SAIS used in Ukrainian army were classified. Table 1 shows that in each category there are information systems and solutions that complement and compete with each other in some way. Most of these solutions are volunteer developments that are at different stages of obtaining documents for official use in the army. However, all of them are already widely used in combat operations [18].

The review of these software solutions allows us to conduct a SWOT analysis of this product segment and identify relevant priorities in its development, prospects, and problems (Table 2). SWOT analysis (or SWOT matrix) is a strategic planning and strategic management technique used to help a person or organisation identify strengths, weaknesses, opportunities, and threats related to business competition or project planning.

The results of SWOT analysis show that the greatest advantage in the development of information systems at different levels of SA is the availability of significant IT potential in Ukraine and motivated developers. A certain decentralisation of activities in the development of SAIS for the military sector gave a significant boost to the formation of a volunteer movement of software development teams. Most of these teams began to form after 2014 and

Table 1. SAIS solutions in Ukrainian army.

System class	Name	Functionalities	Year of development start
Fire Control	'Bronia'	Calculation for artillery firing, terrain orientation	2015
	MilChat	Messaging, broadcasting geo-positions	2018
Tactical level	Ukrop (MyGun)	Calculation for artillery firing and terrain orientation	2009
	'Terminal'	Tactical situation and orientation	2015
Operational level	GISArta	Calculation for artillery firing, targeting, and operations planning	2014
	Kropiva	Calculation for artillery firing and orientation	2014
Strategic level	ComBat Vision	Intelligence, targeting, and decision support	2015
	Delta	Orientation, data exchange, and departmental management	2016
	'Dzvin-AC'	Command and control of combat operations at the command level	2016
	'Virash-planshet'	Gathering, displaying, and analysing air traffic information	2016
	'Prostir'	Management of troops and weapons at the brigade level	2021

Table 2. SWOT analysis of Ukrainian SAIS.

Strengths	Weaknesses
• Modern technological base of development • Integration with NATO-standard data transfer protocols and services • Testing in real-war conditions • Strengthening cyber defence	• Weak communication base in Ukraine • Need to combine different means and forces in combat conditions • Public–private partnership base for development
Opportunities	**Threats**
• Export of technologies • Involvement of professional specialists and teamwork • Attracting external sources of funding • Testing of modern technologies	• Lack of stable sources of funding • Changing conditions for project development as a result of hostilities • Conflict situations with military (state) structures • Subversive activities, cyber attacks on infrastructure

their activities intensified after the outbreak of full-scale war. The teams involved highly qualified specialists. Therefore, the existing software solutions have found a large number of users and are improved constantly. This creates preconditions for the development of software solutions that are competitive not only in Ukraine but may have export potential. Weaknesses include the fact that software solutions are developed mostly autonomously, which means that they are highly dependent on donations for the needs of volunteer teams, and do not coordinate with or compete with other software products. Therefore, the biggest threat is that software developers may face various organisational difficulties, and without systemic support, the results of their work may be lost.

Weaknesses include the fact that software solutions are mostly developed autonomously, which means that they are highly dependent on donations for the needs of volunteer teams and do not coordinate with other software products. Therefore, the biggest threat is that software developers may face various organisational difficulties, and without systemic support, the results of their work may be lost [19].

3.2. Examples of the Most Used Systems

3.2.1. Delta Situational Awareness System

Delta is a system for collecting, processing, and displaying information about enemy forces, coordinating defence forces, and providing SA in accordance with North Atlantic Treaty Organization (NATO) standards, developed by the Defence Technology Innovation and Development Centre of the Ministry of Defence of Ukraine.

Delta is used by very different units. It is a tool for multi-domain operations. This system is used by army, navy, and air defence. Each branch of the armed forces has its own needs and tasks in using Delta.

The Delta system integrates information about the location of enemy forces and assets and allows real-time tracking of the position of enemy troops and promptly recording detected objects for their further fire damage [20]. The system integrates information about the enemy on a digital map, with data taken from various sources: satellite imagery providers, radars, sensors, Global Positioning System (GPS) trackers, and radio intercepts. Users can see what is happening on land, at sea, in the air, in space, and in cyberspace. The system can run on any device: laptop, tablet, or mobile phone. The Delta system was used during well-known operation, such as the defeat of the cruiser Moskva and the liberation of Zmeinyi Island.

The system is used to plan operations and combat operations. The secure ELEMENT messenger, which is part of Delta, is used to coordinate between units and exchange information securely. Delta's platform and services are built to NATO standards, support the Multilateral Interoperability Programme (MIP) specification and allow for NCW. The system is compatible with similar solutions used by the armies of NATO member states [21]. The system was presented during the NATO Tide Sprint event.

Delta is a cloud-based solution and is already implementing NATO standards and the latest industry trends, such as cloud native environment, zero trust security, and multi-domain operations. In NATO member states, such solutions are only at the stage of experimental implementation.

Detla supplants the Soviet principle of information transfer, when an intelligence officer from the grassroots passed information about the enemy to the military leadership. The leadership would make decisions and send them down the chain of command. Such a long path of information slows down the army, and if the command post is destroyed, the possibility of coordination is lost.

In June 2023, Poland hosted the annual NATO CWIX exercise on interoperability of national combat and information systems with NATO systems and protocols. From 18 to 22 June 2023, specialists from the A2724 military unit, as part of a delegation from the Communications Troops of the Armed Forces of Ukraine (J6), tested the Delta Integration Platform for interoperability with similar NATO systems using the state-of-the-art MIP4-IES protocol at the NATO CWIX international exercise in Poland. Currently, only seven out of 28 NATO countries have implemented this protocol and can have all its benefits. Ukraine is among those states that have confirmed the ability to exchange situational information using the modern military exchange protocol. This also gives Ukraine the ability to automatically exchange information with NATO member states during joint exercises and missions. The main protocol tested in 2023 is Link 16. It enables data to be transmitted to Delta from F-16 fighter jets [22].

It is important that the systems on the market are interoperable, and that their developers consider the importance of interoperability at the stage of product development. Delta is just such a system that can exchange data with software solutions from NATO countries. The system interacts with NATO battlefield management systems and operates in accordance with these information exchange protocols [23].

At its core, it is an integration platform designed to ensure that data from various sensors and systems can be collected correctly, and that the Delta user can exchange this information. For example, Delta integrates chatbots developed by the Ministry of Digital Transformation – eVorog and the Security Service of Ukraine – STOP Russian War.

The system is equipped with modern tools for monitoring suspicious activity. Since 2021, allied cyber units have been continuously checking the system for vulnerabilities, unauthorised intrusion attempts, data leaks, etc.

The system is constantly under enemy attack of varying intensity and scale. Separate teams of Russians have been assigned to 'put down' Delta.

Delta developers are constantly learning from the scale of a major war. The priority is to strengthen the system's security. In August 2022, Russians launched a phishing attack on Delta and gained access to two accounts.

For a long time, Delta hid the system from being indexed by search robots so that there were no links to the login page when searching on Google. Hackers faked the resource and raised it in search queries. One of the users took advantage of it and gave their accounts to a phishing site.

The users had access to a limited amount of information about enemy forces in certain areas. The hackers managed to make a recording, but they did not receive complete information about the system's architecture.

Users are checked according to the Security Service of Ukraine protocol, and employees undergo a polygraph. The system has protocols for recognising patterns of suspicious behaviour. Cyber specialists monitor security at all levels – from development to use – 24×7.

Now the developers are faced with the task of providing Fast Identity Online Alliance (FIDO) security keys to all users of the Delta SA system. This is a two-factor authentication tool for accessing various systems and applications. The security key is used in addition to the password as the second factor of user verification. The key is supported by major operating systems and browsers. FIDO is an association of leading technology companies, government agencies, service providers, financial institutions, and payment systems that promotes the development, use, and compliance with authentication standards. The FIDO Alliance has more than 250 members, including such leading companies as Microsoft, Google, Apple, Amazon, Facebook, Mastercard, American Express, VISA, and PayPal. FIDO protocols use standard public-key cryptography methods to ensure stronger authentication. When registering with an online service, the user's client device creates a new key pair. It stores the private key and registers the public key with the online service. Authentication is performed by the client device, which confirms that it owns the private key by signing the call [24].

Semantic data integration takes place on the basis of a mapping framework that displays different data sources. For example, it can be automatic marking when information is taken from sensors in a war zone. Some layers are filled with marks manually: they confirm the information received, for example, about the location of enemy troops, verify it, and give a certain number of participants access to the corresponding layer. The symbols on the map correspond to NATO standards.

After Ukraine's victory, there will be a big question of maintaining the Delta data set, which is a huge resource. This could lead to the corporatisation of the product.

The Delta system has the following export potential:

- compatible with NATO systems,
- hosted in a secure cloud,
- supports integration of different data sources and sensors,
- adapted to the needs of specific types of troops.

In parallel, in 2016, the Ministry of Defence of Ukraine ordered another development from a third-party contractor – Dzvin, a de jure competitor to Delta. Ukrainian army needs a common automated operational-level system for command headquarters to ensure that the troops are covered by the command. The Ministry of Defence tested Dzvin, which was supposed to solve this problem, but the project was frozen in 2021. Prototypes were developed and tested, but encountered bureaucratic obstacles related to the cost of development, time, and product ownership.

It also started to engage foreign companies. The Ministry of Digital Transformation engaged the developer Palantir. The US company with a capitalisation of $16.6 billion has contracts with the CIA, and the US and British defence departments. In Ukraine, Palantir will work with the Ministry of Defence and the General Staff to provide

SAIS of various levels. They help to process and combine information from satellites, drones, and other sources, and make faster decisions.

The functions of Delta in Russia are partially performed by the Acacia-M system, but it is more focused on troop management than on frontline awareness. The Russian Ministry of Defence spent RUB (₽)20 billion ($318 million) to purchase 32 sets of the Acacia-M mobile troop management system in 2018. It is supposed to collect information from other systems for different branches of the armed forces and speed up decision-making at operational and tactical levels.

3.2.2. Operation System Kropyva

The Kropyva tactical command and control system is a software for creating intelligent maps in combination with devices and instruments designed to plan and guide missions. It was developed by Logika Design Bureau LLC, a member of the League of Defence Enterprises of Ukraine.

The development, integration, and testing of the system began in 2014 at the beginning of Russia’s war against Ukraine as a volunteer project, when a group of developers from the Army SOS volunteer organisation began supplying tablets to armed forces. Between 2014 and 2023, 10,000 units of software were installed, and a technical and software support service was set up [25].

The system provides:

- access to an digital map of the area with your own GPS position,
- data exchange with other system subscribers. Data generally includes positions of allied units, coordinates of detected targets, and short text messages,
- solving individual calculation tasks, such as calculating the march, fire area, or artillery corrections,
- ensuring the interaction and transfer of data from reconnaissance assets: unmanned aerial vehicles (UAVs), radar, and sonar systems in an automatic mode.

Equipment required to use the system:

- tablet computer with GPS,
- drone,
- radio station,
- binoculars,
- laser rangefinder,
- thermal imager.

The Kropyva system is used by 90–95% of artillerymen. Kropyva is also used by the Land Forces of the Armed Forces of Ukraine – armoured vehicles, infantry or reconnaissance units, etc. Because of the development, the time to deploy an artillery battery is reduced by fivefold, the time to hit an unplanned target is reduced by almost threefold, and the time to open counter-battery fire is reduced by tenfold, compared to Soviet calculators.

The Kropyva system is an Android application that enters the coordinates of an enemy target, which is received by the nearest artillery battery, which then strikes.

In the course of development, the application has been updated with additional functionality. It updates geometric information about the front line on a daily basis. Soldiers can see where the enemy is and where they are, exchange positions and intelligence, and communicate with the command post. It also includes a navigator, a map with accurate elevations, the distance from one object to another, and the calculation of the range of a gun to an object.

The data from Kropyva is not stored centrally on servers to be streamed to all devices. Each tablet has information only on the positions and weapons it needs.

3.2.3. Bronia System

Bronia is the system that allows firing without a direct line of sight to the enemy. It is used by armoured troops.

When a tank enters a firing position, it has to determine its orientation. This data is transmitted to the platoon commander, who enters it into a tablet application. The parameters of the shells are also entered there and meteorological data is automatically analysed.

The firing positions are calculated at the command post for several tanks simultaneously. For example, for three tanks, this takes 5–7 min, and manually without application, it takes 20–25 min. The commander transmits two parameters of the azimuth pointer and the lateral level to the crew for firing.

The programmers have provided the ability to switch from satellite maps to the general staff maps while retaining information about the targets. The general staff maps show not only that it is a particular road but also the width of the roadway and its surface.

All volunteer solutions were developed on a bottom-up basis, responding quickly to the needs of the military.

3.3. The Situation Centre in the Structure of SAIS

An important component of SA during a military conflict is decision-making based on situational centres. 'Aerorozvidka' unit is developing situational centres that provide SA for all representatives of the security and defence sector at all levels. They are implementing the intelligence, surveillance, target acquisition and reconnaissance (ISTAR) process in Ukrainian army, which has been introduced in NATO countries since the 1990s.

The situation centre is a technological hub that integrates and coordinates intelligence assets and helps to conduct effectively joint operations. Based on this information, headquarters can plan operations much more efficiently, including joint operations involving different units and even agencies. Sharing intelligence assets helps to optimise the resources available to the security and defence forces.

The first situation centre was set up in Kyiv within days of the start of the full-scale invasion. Interacting with the civil–military administration of Kyiv, the situation centre team formed a comprehensive overview of the condition of the city's infrastructure and the region. Coordination was also established between checkpoints and patrols to avoid conflicts over the use of UAVs and the movement of crews near the location of Ukrainian units [26].

The information gathered was used to plan the actions of defenders, establish effective cooperation between different units, and form an operational picture for the leadership of the Ministry of Defence and the military–civilian administration of Kyiv (Figure 4).

Currently, there are eight situation centres in Ukraine; each collects information on its own area of the frontline. The situation centres

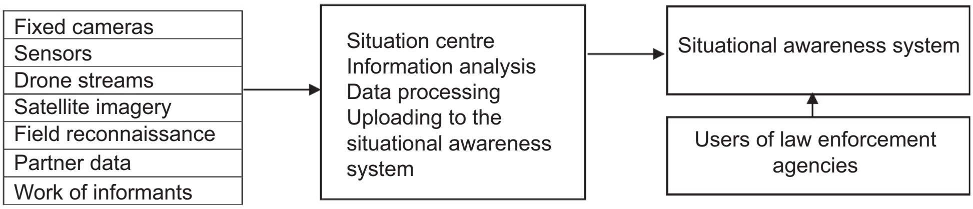


Figure 4. Data analysis model based on the situation centre [27].

are located in Kyiv, Mykolaiv, Kherson, Zaporizhzhia, Kryvyi Rih, Kharkiv, Sumy, Chernihiv, and Donbas. Waging NCW, in which the main advantage over the enemy is achieved in the information component, allows for faster operations, faster management, and greater effectiveness in defeating enemy forces. SA in the context of modern threats is the basis of security, which makes it possible to respond quickly to changes in the situation and have an advantage over the enemy, even with fewer forces and means.

NATO's security system includes the Situation Information Centre (NATO: SITCEN), which provides SA during times of peace, tension, and crisis as well as during strategic exercises. SITCEN receives, processes, and disseminates data from all available internal and external resources. The system also acts as a link to similar facilities in Allied countries and NATO's high command. SITCEN was founded in 1968, but has since been restructured several times to adapt to the demands of the times. Through its various divisions, the centre operates around the clock and provides information to the Alliance's leadership to ensure informed decision-making.

SITCEN Watch provides NATO headquarters with round-the-clock SA of incidents and events around the world. The staff consists of a team of officers and assistants who are on duty in 12-h shifts, 24 h a day, 7 days a week. They monitor and disseminate information and intelligence on the international, political, economic, and military situations, including developments that could affect the Alliance. Watch alerts the relevant military or civilian authorities at headquarters to important developments identified from both covert and open sources.

SITCEN Watch also monitors NATO's ballistic missile early warning systems, supports crisis management organisations and task forces, and assists the NATO security management office in its missions abroad.

The geospatial division provides integrated geographic services to NATO headquarters across land, sea, air, and space. This can range from rapid mapping to providing the most up-to-date overall operational picture. The division also manages geoportals on various networks to build training scenarios during exercises.

The Situational Awareness Integration Team (SAIT), established in March 2020, is dedicated to developing a comprehensive shared understanding of the global and regional security environment and its impact on the Alliance, NATO Allies, and partners. The team contributes to SA by pooling knowledge and expertise and analysing current topics and issues relevant to the Alliance's interests and missions. Among its many tasks, it prepares, coordinates, and hosts the chiefs of staff meeting, which brings together senior officials from NATO headquarters.

The situational awareness integration team also conducts qualitative and quantitative research and brings together stakeholders from across NATO member states. For its research and coordination work, it uses and applies the latest developments in information science.

3.4. Communication Infrastructure

Effective use of the SAIS should not have been possible without the provision of communication infrastructure on the front line. In Ukrainian army, the deployed Starlink system played such a role.

Starlink is a broadband satellite-enabled Internet developed by SpaceX, which makes Ukrainian forces independent from fibre optic cables or mobile networks vulnerable to Russian attack. Currently, there are approximately 20,000 Starlink terminals in Ukraine, most of which are funded by western support [17]. The terminals are crucial for their ability to conduct NCW in Ukraine.

The critical characteristic of Starlink is that its satellite-based design is more resilient towards jamming than regular radio signals. Furthermore, owing to quick installation time, approximately 15 min, Ukrainian forces can maintain a high level of communication without relying on Internet cables. Therefore, access to Starlink hardware is crucial to enhance and sustain Ukrainian NCW capability through the Delta system. In addition, drones use Starlink to keep connected when Ukraine lacks Internet and power because of Russian artillery targeting its critical infrastructure.

As the system highly depends on western support, there is a reason to assume that NATO countries are interested in its operational capability to counter Russian threats.

3.5. Civilian Component of Military Situational Awareness

Since the outbreak of the war, civic initiatives to interactively inform the public about military operations and warn of air threats have developed actively. A number of web and mobile applications are made available to the public to provide SA to the population. Many information elements are implemented in these applications for the first time for civilian purposes. These applications include DeepStateMap.Live, alerts.in.ua, and the mobile applications eTrivoga, AirAlert, and Povitriana trivoga.

3.5.1 Project DeepStateMap.Live [28].

Based on non-profit OpenStreetMaps, DeepStateMap.Live is an interactive online map of the fighting in Ukraine that allows you to follow the changes in the front line and the course of hostilities in the Russian-Ukrainian war. In the spring of 2023, the company launched its own app for Android and IOS.

The map has the following conventional symbols:

- territory de-occupied in the last 2 weeks – blue,
- de-occupied territory – green,
- territory that requires clarification – grey,
- territory captured by Russian troops – red,
- territory of the occupied Crimea and ORDLO – dark red,
- territories of other states occupied by Russia – light pink,
- enemy unit – a unit icon according to NATO standards or a ‘pig’ icon,
- enemy headquarters – the icon of enemy headquarters according to NATO standards or the icon of a tent,
- enemy airfields – an icon of an airfield according to NATO standards or an airfield icon,
- directions of enemy attacks – a red arrow.

You can view the map in different formats. Available map formats are:

- standard,
- topographic,
- satellite.

It is possible to enable the display of fire points based on data from the National Aeronautics and Space Administration (NASA) firms system and compare them with the front line.

Owing to a special mode, it is possible to measure the range of various artillery systems: HIMARS, M777, CAESAR, etc. along the entire front line. A special mathematical modelling of the force of a nuclear explosion of different masses across the map is developed.

The map has a ruler for determining the distance between points in metres. It is possible to build a broken line, which is calculated in total between all points. If the line is closed, you can calculate the area of the created shape. The radiation monitoring points have been added to the map in partnership with SaveDnipro. The application shows enemy fortifications available in open sources since 16 June 2023 [29].

Owing to cooperation with Griselda, an automated military data processing system, on 13 November 2022, the Patogen functionality was launched, which shows modified data on the concentration of enemy numbers along all front lines for civilians, based on classified data. Cooperation with the Griselda system also affects the accuracy of front line mapping, as it allows teams to share operational data. There is a table showing the percentage of liberated and occupied territories since the beginning of the invasion.

There is a closed map functionality for access only to military, with a map of enemy trenches and the ability to calculate azimuth. Since 1 June 2023, regular users have been able to locate their location. A publicly available weather viewer was added on 9 November 2023.

The map of application is widely quoted and used to visualise the fighting in Ukrainian and international media.

3.5.2. Alerts.in.ua

Alerts.in.ua is an online service that visualises information about air alerts and other threats on the map of Ukraine [30].

The main part of the site is a map of Ukraine, which highlights in real time the regions where air alerts or other threats are declared.

The application supports five types of threats:

- air raid alert,
- threat of shelling,
- threat of street fighting,
- chemical threat,
- radiation threat.

Additionally, information about shelling and other dangerous events, such as explosions, demining is published on the basis of media reports.

The service uses the following information sources by default:

1. The official Air Alert Telegram channel from Ajax Systems, which reports airborne alarms and other threats.
2. Official Telegram channels of regional military administrations, public broadcasting, the state emergency service, and their specialised channels for alerting about alarms at the regional level.
3. Official air alert map.
4. Official Telegram channel of the Air Force of Ukraine.

Most of civilian applications are volunteer developments that, if popular, are actively supported by the state government. These apps aggregate data and transform information into a user-friendly form based on cross-platform developments. In parallel, official state channels operate for informing about the situation. Mobile operators support push notifications from the state emergency service of Ukraine. However, government services are often not customer-oriented. Therefore, citizens prefer to use volunteer apps with better interface design and easier usage.

3.6. Cartographic Support

The main basis for the tasks of military and civilian SA is an up-to-date cartographic basis and the use of geographic information systems. Since 2014, Ukraine has been updating the topographic mapping of the eastern regions based on the USC-2000 coordinate system.

With the outbreak of war in 2022, the Ukrainian army faced a shortage of its own mapping data for the northern part of Ukraine. The use of NATO standards in Ukrainian army has led to a transition to using coordinate systems for military cartography based on the WGS-84 coordinate system. Most volunteer projects use open data sources based on non-commercial OpenStreetMaps.

The lack of Ukraine’s own satellite remote sensing data on the territory of Ukraine remains a problem. In particular, an attempt was made to lease a radar satellite from the Finnish company ICEYE to obtain intelligence data. The data operator was the Defence Intelligence of Ukraine. The status of use of this data is currently unknown. Ukraine’s dependence on external sources of high-resolution satellite data complicates the development of SAIS. This is offset by the active use of reconnaissance UAVs of various types at the frontline.

4. Conclusions

During the Russian-Ukrainian war, there was an urgent need to develop various information systems to support SA at different levels of military and civilian management. This has led to the appearance of many volunteer initiatives and the development of state military systems for managing troops. Given the high level of development of the IT sector in Ukraine and the unprecedented scale of military conflict, many solutions in the SA sector have become pioneering and visionary for the military of other countries. In particular, the use of modern web and mobile technologies based on cloud infrastructures, accompanied by advanced encryption and cyber security methods, has become the basis of technological solutions for real-time data exchange.

The second trend was the construction of systems based on NATO standards and the need for effective interaction with the systems, tools, and data warehouses of the Alliance. In Ukrainian army, SAIS are developed at different levels of command and control and include the integration of data from UAVs, satellite imagery, cartography, field data, and intelligence results. SAIS are classified according to four levels of military command: fire control, tactical, operational, and strategic levels. According to their purpose, SAIS are classified by target users, level and geographical dimension of coverage, degree of integration with information and communication platforms, and type of interaction based on them.

The results of the SWOT analysis of software development show a high potential for the development of the existing systems in Ukraine. At the same time, most existing projects are at risk because they do not have ongoing government support. Duplication of work by volunteer teams that do not have joint development management remains a problem.

To date, the most promising systems developed have been Kropyva at the operational and tactical level and Delta at the strategic management level.

A separate mention should be made of civilian initiatives to ensure public awareness, which are divided into military situation monitoring systems and rapid air raid response systems.

Perspective areas for the development of SAIS include standardisation and unification with NATO standards, improving cyber defence and reliability of the systems. The use of systems in real-world combat operations significantly improves their quality of development and creates conditions for further exchange of experience and export of technologies in this area.

The further development of SA systems in Ukraine is to integrate the existing systems, organise an ecosystem of military information systems with the ability to exchange data through secure channels, and a high level of cyber security. From a technological point of view, the development of SAIS is focused on the use of AI tools, big data processing algorithms, methods of forecasting and scenario modelling of changes in the situation [31], and joint processing of ground-based, airborne, maritime, and space-based information sources. From an organisational perspective, products in this segment are aimed at unification and standardisation based on NATO approaches. The process of public–private partnerships continues in this technology sector. There is a high probability that software and solution developers are structured to form vertically integrated structures that may include weapon developers, IT companies, innovation centres, and start-up incubators.

References

[1] M.R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32–64, 1995, doi: 10.1518/001872095779049543.

[2] M.R. Endsley, "Situation awareness in aviation systems," in *Handbook of aviation human factors*, D.J. Garland, J.A. Wise, V.D. Hopkin, Eds., Mahwah, NJ: Lawrence Erlbaum, 1999, pp. 257–276.

[3] M. Endsley. (2001). "Designing for Situation Awareness in Complex System." Proceedings of the Second International Workshop on the symbiosis of humans, artifacts and environment. Kyoto, Japan. [Online]. Available: https://www.researchgate.net/profile/Mica-Endsley/publication/238653506_Designing_for_situation_awareness_in_complex_system/links/542b1ada0cf29bbc126a7f35/Designing-for-situation-awareness-in-complex-system.pdf. [Accessed: Jan. 02, 2024].

[4] A. Munir, A. Aved, E. Blasch, "Situational awareness: Techniques, challenges, and prospects," *AI,* vol. *3*, no. 1, pp. 55–77, 2022, doi: 10.3390/ai3010005.

[5] *Handbook of dynamic data driven applications systems,* E. Blasch, S. Ravela, A. Aved. Eds., Berlin: Springer Cham, 2018.

[6] C. Paul, C.P. Clarke, B.L. Triezenberg, D. Manheim, B. Wilson, *Improving C2 and situational awareness for operations in and through the information environment*. Santa Monica, CA: RAND Corporation, 2018. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2489.html. [Accessed: Jan. 02, 2024].

[7] N.A. Stanton, P. Chambers, J. Piggott, "Situational awareness and safety," *Safety Science*, vol. 39, pp. 189–204, 2001, doi: 10.1016/S0925-7535(01)00010-8.

[8] D. Alberts, R.E. Hayes, *Power to the edge: Command, control, in the information age*. Washington, DC: Command and Control Research Program (CCRP), 2005.

[9] D. Reid, G. Goodman, W. Johnson, R. Giffin, "All that glisters: Is network-centric warfare really scientific?," *Defense and Security Analysis*, vol. 21, no. 4, pp. 335–367, 2005, doi: 10.1080/1475179052000345403.

[10] D. Alberts, J. Garstka, F. Stein, *Network centric warfare: Developing and leveraging information superiority*. Washington, DC: Command and Control Research Program (CCRP), 1999.

[11] V. Garg, T. Wickramarathne. (Nov. 4–7, 2018). "Ubiquitous sensing for enhanced road situational awareness: A target-tracking approach." Proceedings of the 21st international conference on intelligent transportation systems (ITSC), Maui, HI, pp. 831–836. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8569918. [Accessed: Jan. 02, 2024].

[12] M.R. Endsley, "The divergence of objective and subjective situation awareness: A meta-analysis," *Journal of Cognitive Engineering and Decision Making*, vol. 14, pp. 34–53, 2020, doi: 10.1177/1555343419874248.

[13] G. Tadda. (Jun. 30–Jul. 3, 2008). "Measuring performance of cyber situation awareness systems." Proceedings of the 2008 11th international conference on information fusion, Cologne, Germany, pp. 1–8.

[14] W.L. Brandão, M.S. Pinho. (Mar. 18–22, 2017). "Using augmented reality to improve dismounted operators' situation awareness." Proceedings of the IEEE annual international symposium on virtual reality (VR), Los Angeles, CA, USA, pp. 297–298.

[15] J. Lundberg, "Situation awareness systems, states and processes: A holistic framework," *Theoretical Issues in Ergonomics Science*, vol. 16, no. 5, pp. 447–473, 2015, doi: 10.1080/1463922X.2015.1008601.

[16] N. Suri., M. Tortonesi, J. Michaelis, P. Budulas, G. Benincasa, S. Russell, C. Stefanelli, R. Winkler. (May 23–24, 2016). "Analyzing the applicability of internet of things to the battlefield environment." Proceedings of the international conference on military communications and information systems (ICMCIS), Brussels, Belgium, doi: 10.1109/ICMCIS.2016.7496574.

[17] R. Oscar. (Feb. 03, 2023). *Network-centric warfare in Ukraine: The delta system*. [Online]. Available: https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system. [Accessed: Jan. 02, 2024].

[18] T. Melnyk. (Feb. 04, 2023). *Delta military software is now officially in the Ukrainian armed forces. It helped in all major operations – from the sinking of the Moskva to the liberation of Zmiine. Why it is faster to fight with it.* [Online]. Available: https://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta-dopomagav-u-vsikh-velikikh-operatsiyakh-vid-potoplennya-moskvi-do-zvilnennya-zmiinogo-chomu-z-nim-zsu-voyuyut-shvidshe-07122022-10318. [Accessed: Jan. 02, 2024].

[19] T. Melnyk. (Nov. 14, 2022). *IT chaos in the service of the armed forces. Hundreds of thousands of military personnel use various software developed by volunteers. Is such decentralisation dangerous?* [Online]. Available: https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700. [Accessed: Jan. 02, 2024].

[20] F. Yura. (Jun. 14, 2023). *How the Delta software works and why the offline approach does not work in the army – An interview with the head of IT at Aerial Intelligence.* [Online]. Available: https://dou.ua/lenta/interviews/delta-and-it-in-the-army. [Accessed: Jan. 02, 2024].

[21] Militarnyi. (Oct. 27, 2022). *Ukraine unveiled its own Delta situational awareness system*. [Online]. Available: https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system. [Accessed: Jan. 02, 2024].

[22] ArmyInform. (Jul. 12. 2023). *Ukraine's Delta situational awareness system passes NATO tests and can integrate F-16 fighters.* [Online]. Available: https://army-inform.com.ua/2023/07/12/ukrayinska-systema-sytuaczijnoyi-obiznanosti-delta-projshla-vyprobuvannya-nato-i-mozhe-integruvaty-vynyshhuvachi-f-16. [Accessed: Jan. 02, 2024].

[23] J.M. Pullen, S. Carey, U. Schade, O.M. Mevassvik, S. Galan, L. Khimeche, S. Godoy, M. Powers, N. Cordonnier, N. de Reus, N. LeGrand. (Feb. 11, 2008). *NATO MSG048 coalition battle management initial demonstration lessons learned and way forward*. [Online]. Available: https://repository.tno.nl/SingleDoc?find=UID%20 59169081-fa5c-4d0e-a46c-64ac3eaaaf13. [Accessed: Jan. 02, 2024].

[24] Ukrinform. (Apr. 04, 2023). *The armed forces of Ukraine told how the military uses the Delta platform.* [Online]. Available: https://www.ukrinform.ua/rubric-ato/3731063-u-zsu-rozpovili-ak-vijskovi-vikoristovuut-platformu-delta.html. [Accessed: Jan. 02, 2024].

[25] T. Melnyk. (Jul. 24, 2023). *Stinging Nettle. How Ukrainian software for artillerymen affects the course of the war*. [Online]. Available: https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054. [Accessed: Jan. 02, 2024].

[26] Ukrainska Pravda. (Sep. 24, 2015). *Innovations for the army. Bronia programme for tankers*. [Online]. Available: https://life.pravda.com.ua/volunteers/2015/09/24/200649. [Accessed: Jan. 02, 2024].

[27] Aerorozvidka NGO. (Jul. 11, 2024). *Unmanned aerial vehicles, situational awareness,* cybersecurity. [Online]. Available: https://aerorozvidka.ngo. [Accessed: Jan. 02, 2024].

[28] DeepStateMap.Live. (Mar. 12, 2023). *Map of military operations*. Available: https://deepstatemap.live. [Accessed: Jan. 02, 2024].

[29] SaveEcoBot. (Jun. 16, 2023). *Radiological maps in Ukraine online*. Available: https://www.saveecobot.com/en/radiation-maps. [Accessed: Jan. 02, 2024].

[30] Alerts.in.ua. (Mar. 18, 2023). *Map of trivog Ukraine*. Available: https://alerts.in.ua. [Accessed: Jan. 02, 2024].

[31] V. Putrenko, N. Pashynska, "Analysis of regional armed conflicts using spatial clustering methods," *Lecture Notes in Information Sciences*, vol. 9, pp. 67–73, 2020.

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?

Marina Miron | War Studies, King's College London, UK |
ORCID: 0000-0003-3695-6541

Rod Thornton | Defence Studies, King's College London, UK |
ORCID: 0000-0002-9566-8956

Abstract

This article examines the Russian military's Information Warfare (IW) activities. The particular focus here is on the use by this military of operations in cyberspace as a strategic force-multiplier. It seeks to shed light on why such operations are so important to this military and what goals it hopes to achieve through their use. In particular, this article highlights the role played by what Russian analysts refer to as cyber-psychological and cyber-technical operations. Having established the background to the Russian military's IW thinking, this article then goes on to examine the application of its cyberspace operations against Ukraine: both before the 2022 invasion and as part of it. It is from this examination of the cyber-attacks conducted against Ukraine that a better understanding of the potential of Russian IW can be generated. As such, lessons can be drawn from this conflict as to how, in the future, the Russian military might employ IW specifically against NATO states as part of a major kinetic confrontation. But, as this article notes, drawing lessons as to the actual strength of Russian IW capabilities from the Ukraine conflict may be a flawed process. It may be the case that the Russian military might not have shown its true cyber hand in

Received: 21.03.2024

Accepted: 23.05.2024

Published: 08.07.2024

Cite this article as:
M. Miron, R. Thornton "The use of cyber tools by the Russian military: Lessons from the war against Ukraine and a warning for NATO?," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190142

Corresponding author:
Marina Miron, War Studies, King's College London, UK. E-mail: marina.miron@kcl.ac.uk;
0000-0003-3695-6541

Ukraine. It may be saving its best cyber tools for any future conflict with NATO itself.

Keywords
cyberattack, cyberspace operations, information war, Ukraine, Russia

1. Introduction

It has long been understood that when it comes to its confrontation with NATO states, the Russian military has been looking to operations in cyberspace to provide for significant force-multiplier effect [1–3]. Such operations offer to have this effect in two specific areas: in the realm of ideas and that of technology. The Russian military – perhaps the most important Russian actor engaged in 'malign' cyberspace activity against NATO states – refers to these two realms as the 'cyber-psychological' and the 'cyber-technical' [4]. The former realm uses cyber means to conduct influence operations by playing on the consciousness of targets, while the latter variant aims at disrupting, degrading, or destroying the IT systems of targets. Such operations, in whatever realm – and as this article explores – are perceived by the Russian military to be vital tools in both the ongoing peacetime 'competition' [5] between Russia and NATO states and any actual kinetic operations that may at some point transpire; that is as part of major armed conflict between the two [6]. This article seeks to highlight just how important these cyberspace operations are, in particular, to the Russian military. It first provides the conceptual basis behind this military's emphasis on such operations and then goes on to discuss some specific examples of their use. The focus where the examples are concerned is on those cyberspace activities sourced to Russia that have been used against Ukraine since 2014 and specifically during the war that began in 2022. From such an analysis, this article then sheds light on the specific Russian cyber capabilities that may, in the future, threaten NATO states and the Alliance's ability to prevail in any potential future war with Russia.

2. Conceptual Basis

It can be said that in Russian thinking 'information' has a much larger role to play as a tool of 'warfare' (however understood) than it does in the West. The notion of using information for propaganda purposes during wartime dates back to Tsarist times [7]. However, the more refined idea of using information as a strategic tool to generate major effect against state rivals first really began to be discussed in the later Soviet period. In 1960, Evgenii Messner in his book, *Myatezhvoyna* (*Rebellion war*) was one of the first to look upon ‘information warfare’ (IW) (or, in Russian, *informatsionnoe protivoborstvo*) as a true strategic-level weapon [8]. Mere information, applied adroitly, could be weaponised by influencing the consciousness of an adversary state’s population to incite the said ‘rebellion’ against its own government. By such means, that government could be brought down and replaced by one more amenable to Moscow. In essence, that state would have been ‘defeated’.

Of those Russian thinkers who followed in Messner’s footsteps in terms of this thinking about the power of IW, Igor Panarin stands out. In 1997, Panarin obtained his doctoral degree in political science with a dissertation entitled, *Information-psychological support of Russia’s national security* [9]. And while it is difficult to determine the scope of the overall influence his writings have had on the recent practice of Russian IW, it should be noted that Panarin’s methodological framework for the theory of IW came to serve as the capstone for the Information Security Doctrine of the Russian Federation of 2000 [10].

It was Panarin – now operating in the era of IT systems – who first divided IW into two distinct types: the ‘information-psychological’ and the ‘information-technical’. According to Panarin, these two forms differ in terms of their target sets. The first, the information-psychological, looks to influence two particular systems: the system of elite decision-making and the system that relates to public consciousness and thus to the forming of public opinion. This latter system can then go on to influence elite decision-making as a second-order effect. In terms of directly influencing the decision-making of state elites, the targets can range from those at the politico-strategic level right down, in the military sphere, to leaders at quite low levels in the armed forces [11]. The ultimate objective, as Panarin [11] points out, is to generate *manipulation* at the very highest level possible; that is, ‘to force the leader of the opposing side to act according with the goal of information war’. This form of IW has now come to be known in Russian circles as the ‘cyber-psychological’. This is because the information being supplied to generate the required manipulation will more than likely be coming across IT means.

The fact that, in theory, significant outcomes can be generated at the strategic level through the use of *mere* information has, as noted, attracted an audience in the Russian military. For this military, information appears to offer the enticing possibility of actually winning 'wars' without kinetic engagement. This is important for a Russian military that has, certainly over the last 20 or so years, understood that it cannot hope to prevail against NATO forces in any major conflict. It is not strong enough in conventional military terms and it would have, it understands, to resort to nuclear weapons to stave off defeat by NATO [12–14]. This is viewed as distinctly undesirable [15]. Hence, the Russian military has accepted that it has to look to asymmetric means – such as IW – if not to actually win its wars with NATO, then at least to gain strategic advantage vis-à-vis the Alliance [2, 16]. The second impetus behind this focus on IW is the view that the Russian military must, as it sees it, match and defend itself against NATO's cognitive technologies which could help NATO achieve a strategic victory, as the adviser to the Russian Defence Minister, Andrei Il'nitsky has suggested [17, 18].

Very senior Russian military officers have not only come to understand the power of IW but also to actively advocate its use. General Yuri Baluyevsky, the former head of the armed forces (from 2004 to 2008), was one of the first such senior officers to stress that trying to win an information war was more important than trying to win a classical military confrontation. The fact that information could be used to produce significant effects against 'the principal organs' (the 'elite decision-makers') of an enemy state was a major attraction to him [19]. The current (as at March 2024) Chief of the General Staff, General Valerii Gerasimov, has further elevated the importance of IW as a weapon of significant influence. He first pushed its capabilities in a speech he made in 2013. This was summarised in his important article entitled, 'The value of science in foresight' [20]. Similarly, influential senior serving, or retired military officers have been repeatedly arguing in Russian military publications that the main focus of peer-state warfare should be placed on destroying adversary states from *within* using non-kinetic means, such as IW, instead of trying to achieve such destruction by kinetic means [21, 22]. Colonel (ret.) Aleksandr Barthosh [23, 24], in particular, has proved influential. He has underlined recently the importance of using information to shape the belief systems of an adversary state's population. As Bartosh [23] puts it, 'the objective is to manipulate the enemy state's population's beliefs'. Such beliefs will then go on to drive the decision-making of the aforementioned elites. He also looked at the way information could influence the 'consciousness' (i.e. the morale) of an adversary state's armed forces personnel. His ideas were building on not just those presented earlier by the likes of Messner and Panarin but also those of Sergey P. Rastorguev [25]. But Bartosh [23] has perhaps more elegantly understood that the power of IW applied at the strategic level comes from *combining* influence operations deployed against the mindsets of an adversary's civilian population with those directed at the state's civilian and military leaders.

It is through the work of this series of influential Russian observers (and many others not mentioned here) that the power of IW as a tool of warfare has become so ingrained in Russian military thinking. And certainly, this IW tool has become a part of such military thinking in ways that are not mirrored by NATO militaries: these tend to focus almost exclusively on generating kinetic effect, rather than non-kinetic effect [26]. For instance, current Russian military doctrine refers to the important role that inciting 'the protest potential of the population' plays as a strategic tool (and it would, of course, be incited through the use of IW techniques) [27]. No NATO military doctrine would ever include reference to such a technique.

Today, of course, the inciting of such 'protest' is far more easily generated given the role that social media now play in modern societies. Misinformation and disinformation can be disseminated very easily across such media that aim to discredit western institutions (including NATO) and to sow doubt and confusion about individual western government's means of/right to control their populations. False narratives can also act to amplify the existing societal divisions that serve to create damaging schisms. Social media also represent a convenient avenue of attack to weaken the unity of NATO and ultimately to advance its own geopolitical and military interests [24, 28–30]. Moreover, all of this targeting can be done today very easily across IT systems [2].

Here then is the power of the cyber-psychological tool. However, there is also the profound power today of the cyber-technical form of attack. Such attacks target data transmission systems [11]. They can serve to disrupt, deny, or degrade information flows that enable everything from the effective functioning of adversary states' critical national infrastructures (CNIs) down to interfering with their militaries' battlefield systems at the tactical level. Russian analysts, however, tend to concentrate on the *strategic*-level application of cyber-technical means, given that they can also, like the cyber-psychological tools discussed above, generate major strategic – perhaps, indeed, war-winning – effects. Fundamentally, major cyber-technical attacks can also be used with the aim of calling into question the ability of any targeted state to be effectively governed [28, 31–33].

As several Russian sources also affirm, ideally strategic-level cyber-psychological operations should be employed in *coordination* with strategic-level cyber-technical attacks. The hope is that synergies would be created that maximise effect. According to Panarin [11], '...sometimes the methods of information and technical influence are carried out in combination with the methods of information and psychological confrontation.' Moreover, and of course, by using cyber-based means, these effects can be generated, as the likes of Rastorguev [25] point out, in an extremely resource-lite and cost-effective way.

It is this coordination, this combination of the two forms of attack that is seen as key in generating the degree of dislocation that can actually undermine adversary state governments from 'within'. The goal is to create what Bogdanov and Chekinov [22] refer to as 'chaos' within any targeted state. Examples here might be long-term cyber-psychological activity designed to undermine a state population's faith in its own government which is then allied to and exacerbated by attacks on that state's CNI that create major disruption to everyday life (lights going out; no Internet; banks not functioning, etc.). Power grids would here be a particular focus for cyber-technical attack [34]. The popular discontent resulting from both forms of attack may then incite the 'protest potential of the population' that could bring down the government – to be replaced, of course, by one more suited to Russian strategic interests. Another example of coordinated action would be the use of cyber-technical means to undermine faith in the voting count in, say, the general election of a NATO state, while at the same using cyber-psychological means to call into question the right of the winner of that election to govern – inventing a political scandal, for instance. This may undermine freely elected governments. An example here might be the Russian coordinated cyberattacks using the two forms that sought to materially affect the French presidential election of 2017 [35].

This attack on the French election was seen to be the work of the GRU's (*Glavnoye Razvedyvatel'noye Upravleniye*) Military Unit 26165 or FancyBear [36]. The GRU is the principal intelligence arm of the military. Russian cyberspace operations against adversary states – using both cyber-psychological and cyber-technical variants of attack – are also engaged in by the internal security force, the FSB (*Federalnaya Sluzhba Bezopasnosti*), and the foreign intelligence service, the SVR (*Sluzhba Vneshney Razvedki*) [37]. The GRU, being the most potent and aggressive of these three, is seen, moreover, to be the controlling body that coordinates cyberspace operations of both FSB and SVR [38]. Obviously, and particularly when mass effect is called for (such as with distributed denial-of-service [DDoS] attacks), these three agencies can call on assistance from Russian civilian hackers – whether voluntary or forced. Other, non-state actors, such as the Wagner Group (and its successors) can also contribute [38, 39].

Overall, when looking at this issue of Russian IW and how to operationalise it through cyber means, it needs to be understood just how much emphasis that the Russian military is putting on it as a strategic tool – and as, indeed, a potentially war-winning tool. As Margarita Simonyan, the then editor-in-chief of *Russia Today*, put it even back in 2013, '...information weapons are comparable to weapons of mass destruction' [40]. After 10 years, this mindset might be seen to apply even more, given the across-the-world increasing reliance on IT systems and the rise of social media. This said, however, the question for NATO and its constituent states – which are seemingly the main targets for Russian military IW – is, can these cyber-psychological and the cyber-technical operations really work to generate the effect that Russian analysts and observers have been advertising? Just how effective can these IW means of 'warfare' be against NATO if ever they were to be employed synergistically against NATO states at times of high geopolitical tension and particularly as part of any major kinetic conflict? This is one of the major questions that NATO countries must be asking – and are asking [41]. In light of such questions, it seems apposite to gauge some sense of the threat posed to NATO by looking at Russian activities in this IW field that have played a part in Moscow's conflict with Ukraine since 2014.

3. Russian Cyberspace Operations in Ukraine prior to the 2022 War

In the years before Russia's full-scale invasion of Ukraine in February 2022, Moscow's exponents of offensive cyber engaged in several significant operations designed to serve strategic ends and which were an adjunct to kinetic activities. For instance, the GRU's Military Unit 54777 (also known as the 72nd Special Service Centre) [42] was known to be crafting an anti-Chechen information campaign during the 1990s. There were also both cyber-psychological and cyber-technical attacks against Georgian targets conducted by GRU's Unit 74455 (Sandworm) that were part of the Russian invasion in 2008 [43]. More recently, Unit 54777 also came to be involved in shaping the information environment prior to Russia's annexation of Crimea and later seizure of the eastern Donbas in 2014. This was done using two of Unit 54777's front organisations, namely, InfoRos and the Institute of Russian Diaspora. The aim was to create an impression that Russian speakers in the regions in question wanted Moscow to intervene to help them [44]. Thus, as expected and given the emphasis of the writings on this subject over the last several years, Russian IW – using both cyber-psychological and cyber-technical elements – has had a significant role to play as part of the kinetic conflicts being conducted in the service of Moscow's strategic interests.

However, in considering the use of IW to run alongside such kinetic operations, it must be remembered, of course, that the Russian state, before the initiation of such operations, will also have been engaging in what might be looked upon as more long-term preparatory activity in the cyber-psychological realm. There will have been a kind of 'softening-up'/'preparing the ground' process designed to reduce opposition in any targeted area/state. Such preparatory cyber-psychological operations can also, of course, be used in tandem with long-term cyber-technical attacks. Such a combination can clearly be noted when considering Russian cyberspace operations against Ukraine before 2022. There were noted to be dozens of significant cyber-psychological attacks in the months preceding the invasion [45] and several major cyber-technical attacks, chiefly targeted at Ukraine's CNI, notably its power grid [46].

Among the most significant of the pre-2022 cyber-technical operations were those conducted by the Sandworm group. This is also a GRU entity and otherwise known as Military Unit 744551 or Voodoo Bear. It works out of the GRU's Main Center for Special Technologies (*Glavnyi Tsentr Spetsial'nykh Tekhnologii* or GTsST). This unit has been linked to some of the most destructive cyberattacks worldwide [47]. It was Sandworm that stood accused, along with a range of cyber-espionage activities, of conducting the cyberattacks against Ukraine's CNI (particularly its power grid) that began soon after the Euromaidan demonstrations in Kyiv in 2014. The most prominent of these were the BlackEnergy3 attack in 2015 (exploiting Microsoft Word's macro-feature) and the Industroyer malware applied in 2016 [46, 48]. One of the best-documented instances, however, of Sandworm's activities was its deployment of the notorious NotPetya malware in 2017. Although Ukrainian CNI was the initial target, the virus involved spread to create damage to IT systems worldwide, including in Russia itself. Major financial losses were incurred both within Ukraine and internationally, most notably by the Danish Maersk shipping company [49]. The work of Sandworm demonstrated a notable level of sophistication, marked by coordination of a series of attacks and by meticulous consideration of potential mitigation activities engaged in by the targeted entity [46, 48].

The GRU’s Fancy Bear group was also engaged in significant cyber operations prior to the war. Most prominent were those designed to interfere with the everyday lives of as many ordinary Ukrainians as possible. Spearphishing, brute-force, and ‘password spraying’ attacks targeted individuals’ accounts [50]. The SVR’s CozyBear unit also conducted cyber-attacks against the Ukrainian military, political parties, diplomatic agencies, think tanks, and non-profit organisations during the conflict in Ukraine.

By the beginning of 2022, it could be said that Ukraine had been subjected to a series of cyberattacks from a variety of Russian agencies that were looking to create a sense of political and societal dislocation to weaken the bonds that held the country together. To exacerbate the situation, and just before the February 2022 invasion, Russian cyber-technical attacks against Ukraine ‘soared’ [51]. This is what should be expected as part of any prelude to an actual Russian kinetic attack (it was the case in Georgia in 2008 as well). By the middle of February 2022 (with the invasion itself beginning on 24 February), cyberattacks were bringing down the websites of Ukrainian government departments and data-wiping malware was being used against over 100 commercial enterprises. In line with the thinking of Bogdanov and Chekinov, the aim was said to be to sow a degree of ‘chaos’ within the country [51].

4. Russian Cyberspace Operations during the 2022 War

According to Russian doctrinal approaches, it would, of course, be expected that the actual movement of Russian troops across the Ukrainian border on 24 February 2022 would be accompanied by significant cyberspace activity. This would contribute to the generation of disruption and dislocation – if not actual chaos – which would assist the movement of troops on the ground and the gaining of strategic objectives.

When looking specifically at Russian operations in the cyber-technical realm, it will doubtless be the case that the Ukrainian authorities (and NATO itself) would not want to advertise any successful (or even unsuccessful) hacks into Ukrainian military IT systems. This would be sensitive information that would need to be kept from the Russians in order to make, in effect, their battle-damage assessment (BDA) in this cyber-technical realm more difficult to quantify. Given this situation, providing a true analysis of actual Russian hacking activities in this field is difficult.

This said, however, there were known major cyber-technical attacks in the initial period of the invasion. Of note in this regard was the ViaSat KA-SAT hack, which could hardly be hidden. This took place just before the invasion began and was patently designed to be coordinated with it [52]. It was an attack on the downlink ground terminals of the ViaSat satellite network serving Ukraine [53, 54]. While affecting millions of civilian users in Ukraine (and across eastern Europe), it also, crucially, denied information, surveillance, command and control, and communication means to Ukrainian forces and acted to limit their operational capabilities [55]. This did create a military advantage for Russian forces [56].

The use of such cyberattacks so early in the invasion would, as can be understood, be designed to have two particular effects in the strategic realm. Both relate to the sowing of confusion, the generation of chaos. Certainly, the ability of the Ukrainian armed forces to function effectively as a counter to the invasion would be one. However, government structures would also be a target. The Kyiv authorities needed to be seen to be in control in the invasion's early stages when rumours and counter-rumours would be running rife. Slow government reaction – such as in terms of reassuring the population and to creating a sense of the state itself still actually existing – could be fatal in any invasion's first few hours. Anything, thus, that interfered with the ability of both military and government to act quickly would allow scope for a vacuum of control to exist which Russian forces could take advantage of. For in such an invasion as this, the prime goal for Moscow would be to try and have its forces seize the seat of government and impose a Moscow-appointed administration as soon as possible. Anything that would slow down the reaction of the Kyiv authorities – military and government – would work to Moscow's advantage; and here both cyber-psychological and cyber-technical attacks can be seen to have had a role to play.

As it happened, the government in Kyiv was able to maintain control. An attempted FSB *coup de main* operation to seize government structures in the centre of Kyiv on the first day of the invasion was thwarted. Also blocked in the first few days was an attempt to seize Hostomel airfield, close to Kyiv, by Russian Airborne Forces (VDV). This prevented any push by these VDV to the centre of Kyiv and thus to gain control of the capital [57]. Ukrainian forces retained enough command-and-control and coordination capacity to at least hold back this initial assault. Hence, it may be said that whatever Russian cyber-technical attacks were applied in this initial period were not successful: the degree of Ukrainian control was greater than the degree of chaos that Russian cyberattacks attempted to generate.

In the cyber-psychological realm, there were a number of attempts, in the invasion's early days, to deploy misinformation and disinformation that targeted the consciousness of the Ukrainian population [58]. Particular aims were to undermine support for individual political and military leaders. Their reputations and their right to control the government/armed forces were called into question [59]. Note should be taken, in this regard, of one particular operation conducted by the Russians. This could have proved very telling in the conflict's initial stages. This was the creation of a deepfake of Ukrainian President Volodymyr Zelensky. It appeared on 16 March 2022 in a video on Facebook and YouTube. Deepfakes are a combination of both cyber-psychological and cyber-technical means. The idea behind them is to artificially generate an image/video of a particular leading or influential figure – one of the elite decision-makers – and to have 'them' be seen as acting in ways that suit, in this case, Moscow's ends. The deepfake of Zelensky had 'him' making a speech in which he was calling on Ukrainian troops to 'surrender' [59]. Here, writ large, is the kind of effect that the Russian proponents of IW would see as its ability, using such as this deepfake tool, to have a major strategic, indeed, war-winning effect. If this deepfake had actually gained traction among the Ukrainian population/military, then it could have led to the country's defeat. As it happens, it did not. This was, in part, down to the fact that a few days before the video appeared, Ukraine's Center for Strategic Communication had warned that a deepfake of Zelensky would appear. The authorities were thus prepared for it, and it could be countered. But what this deepfake lacked most of all was veracity; it did not look 'right'. It was clumsy and maladroit. Still, though, Zelensky was forced into making a 'real' appearance and to deny it was 'him' [59]. Beyond its clumsiness, what also seems to have been a mistake here is that this deepfake only made an appearance a few weeks into the war. If it had appeared in the first few hours, or at least the first few days when the situation was at its most 'chaotic', then it could have had more effect within the general confusion pervading at that time.

Beyond the cyberspace operations that were evident in the initial days and weeks of Moscow's 'special military operation', many more have continued throughout the conflict. A particular increase in their use was noted from January 2023 onwards [6]. The GRU's Sandworm group has resurfaced several times. Where this body is concerned, Mandiant Intelligence has documented the consistent deployment of a standardised and replicable common set of tactics, techniques, and procedures (TTPs) employed during the conflict [60]. A GRU ‘playbook’ has been seen to be at work. Despite an extended period of aggressive and high-tempo operational use, this playbook appears to have exhibited remarkable resilience. There are five noted elements in this playbook:

1. *Living on the edge*: Here, there is exploitation of compromised edge infrastructure, such as routers, virtual private networks (VPNs), firewalls, and mail servers where interventions are challenging to detect.

2. *Living off the land*: In this approach, there is the employment of inherent tools, such as operating system components or pre-installed software, which can be used for activities such as reconnaissance and information theft. The malware footprint is minimal, which means detection is often difficult.

3. *Group policy objects* (GPO): Here, the policy settings within file systems are targeted, enabling the deployment of wipers through GPOs.

4. *Disrupt and deny*: With this technique, ‘pure’ wipers are utilised alongside other low-equity disruptive tools, such as ransomware, tailored to various contexts and scenarios to disrupt and deny targeted systems.

5. *Telegraphing success*: Where cyber-psychological operations have attained a degree of success, this tends to be amplified through a series of hacktivist personas on Telegram (widely used in Russia).[1]

In terms, specifically, of cyber-technical attacks, there is also evidence of their being combined with kinetic activity. In October 2022, for instance, Sandworm orchestrated a cyber-induced blackout of Ukraine’s power grid concurrently with kinetic missile strikes (from the Air Force) on elements of this same grid. Details of the cyberattack were disclosed by Mandiant, which emphasised Sandworm’s use of a ‘living off the land’ (LotL) approach (see above) [61]. In this case, previously planted data-destroying wiper malware, which had evaded detection, was activated once the missile strikes on the grid had gone in. Sandworm’s malware erased data content across the utility’s network that hindered any repair of the initial damage. The blackout thus lasted longer [62].

[1] Adapted from [60].

This particular above example is indicative of the type of attack that seeks to create the synergies that Panarin first called for in his idea of fusing cyber-technical and cyber-psychological operations. What initially looks like a cyber-technical operation can be seen to morph into a cyber-psychological operation, given the effects that it subsequently can create. The overall Russian aim – where a series of attacks on CNI is involved – would be to sap civilian morale that then leads populations to look to their government to seek an end to their suffering – that is, to call an end to the war. In a similar vein, on 12 December 2023, there was a large-scale cyberattack on Ukraine's mobile phone provider Kyivstar. This left more than 24 million subscribers without cell phone services for several days [63]. Kyivstar subscribers were also unable to manually change their data connection to that of another provider, meaning they were only able to purchase SIM cards from other providers, causing large queues [63]. Around 1.1 million people live in remote locations in Ukraine where Kyivstar is the only provider available [63]. Again, creating such an outage would be geared to undermining the population's capacity to put up with the exigencies of the war.

The above Sandworm example is also indicative of the ability of Russian hackers to adapt and to evolve their forms of attack. Over the course of the conflict, Sandworm's tactics have changed from using highly customised malware (such as the Industroyer malware used to target CNI in real time) to the use of more agile LotL techniques [62]. Another example of cyberspace adaptation is that conducted by another GRU hacker entity known as Cadet Blizzard. This was first identified by Microsoft in June 2023 [64, 65]. This group, operating without bespoke malware, functions as a conventional network operator, seeking public signals to disrupt with the overall aim of generating morale-sapping intimidation. It engages in the likes of website defacements and hack-and-leak operations. It has been targeting not just Ukraine but also NATO member states supporting Ukraine [66]. Microsoft's report identifies Cadet Blizzard as a significant actor in the Russian cyber threat landscape [66]. The examples of Sandworm and Cadet Blizzard indicate that the Russian agencies involved in cyberspace operations can be seen as adaptive, as learning organisations [67].

All this said, however, when looking at Russian offensive cyber activities in the war in Ukraine, it should be noted that they have not been as devastating as might have been expected. Given the noted emphasis in Russian military circles on the importance of offensive cyber as a tool of warfare – and given the noted capabilities that Russia appears to have in the cyber realm [68–70] – the number of hacking attempts and their sophistication during this war has been, perhaps, limited. They have not proved as damaging as was predicted by many observers before the war [71]. This may be the result of an overestimation of the likes of the GRU's capabilities. It may also be down to stronger than expected Ukrainian cyber defences (which had been honed with the assistance of NATO countries since 2014) [72]. However, there is also a further possible cause here. This is that Russia may be wanting to basically 'hide' its true cyber capabilities in this Ukraine war because it does not want to show them to its NATO adversary. It may be holding these capabilities back to save them for a much more important future conflict with NATO. If NATO were to be forearmed about the real extent of Russian cyber expertise, by witnessing them being used against Ukraine, then NATO could develop its own defences. As Kofman et al. [73] expressed it, 'high-end cyber capabilities may have been held in reserve for conflict with the United States and NATO'.

5. Cyberspace Operations against Satellites

One characteristic of Russian cyberspace activities during the war, and one which should have specific resonance for NATO planners, has been the attacks against satellite links. Such links have to pass through the IT systems of ground stations and so they can be vulnerable to hacking. Data to or from any satellite can be blocked, corrupted, or spoofed. Moreover, the actual movements of individual satellites or even whole arrays can be controlled through cyber intervention [74]. This can 'induce harmful satellite manoeuvres' [75]. As David Burbach sums up, 'an invulnerable satellite fleet [up in orbit] is irrelevant if cyberattacks can impair its ground-based control systems and user access' [76].

The Ukrainian military has made much use of western satellite feeds (for navigation, guidance, communications, etc.). The Ukrainian population has also been looking to satellite-supplied data to aid in the conduct of their everyday lives. The temptation for Russian hackers to target satellites is therefore great – resource-lite cyber-attacks can produce some profound results. It is not only the GRU involved here in such anti-satellite (ASAT) attacks but also, it seems, affiliates, such as the 'cyber troops' of the (former) Wagner organisation [77]. The ViaSat hack in the first few days of the invasion has been mentioned above but there have been other notable examples. Elon Musk's Starlink system of satellites was also, for instance, subject to hacking attempts [78].

It appears, though, and as with wider Russian cyberspace operations, that the degree of attempted hacking of satellite links during the war has not been as high as might have been expected [79]. This may, again, be a case of overestimating capabilities or that Ukrainian cyber defences are better than expected. And it may also be because Russian cyber capabilities in this field are being husbanded for use in a future major war. However, other specific issues are also involved here. Firstly, the Russian economy, at least to some degree, itself relies on the data supplied by western satellites. Russian high-tech industries look, in particular, to the Global Positioning System (GPS) to provide a very precise timing mechanism. Such a benefit appears to be restricting Russian cyber-interference with the GPS. This does mean that GPS-guided Ukrainian missiles and drones are not being prevented from hitting their targets, including within Russian territory. Additionally, the Russian military itself also looks, in part, to GPS for navigation and guidance and would be hindering its own capabilities if GPS became subject to a cyberattack [80].

This issue, though, of the hacking of satellite systems could be a major problem for NATO in any future major conflict with Russia [81]. A host of NATO capabilities that outmatch those of the Russian military (mostly related to C4ISR and weapons' guidance) rely on unfettered access to satellite signals. If these signals are interfered with, then it could profoundly affect NATO's military strength. Given what is at stake, Russia will inevitably be involved in what a leaked report from the US Central Intelligence Agency noted that China was already doing. Beijing was said to be 'building cyber weapons to hack into enemy satellites that would render them useless during wartime' [82].

6. A Warning to NATO

Beyond the issue of its satellites being potentially 'rendered useless' by Russian hacking, NATO states could (will?), in the future, be faced by much wider threats from the Russian military's use of IW applied over cyber means. This military is one, as noted, that looks upon IW as a major force-multiplier to a degree that NATO does not. The Russian military has a specific focus on how cyber-psychological and cyber-technical operations can be utilised to create strategic, perhaps even war-winning, effect. The cyber-psychological methods generally look to generate the long-term undermining of state adversaries; to weaken them from within using influence operations. The cyber-technical means will, in peacetime, largely be looking for weaknesses within western

IT systems that can be exploited later and used especially during actual kinetic conflict. Ideally, according to Russian thinking and when necessary, the two methods – cyber-psychological and cyber-technical – can be combined to create synergies of effect. This would be seen as especially productive in the very early stages of any major kinetic conflict when the coordinated activities of the two types could, at least theoretically, produce strategically important results.

There are a number of issues which NATO states should be specifically aware of in regard to future Russian offensive cyberspace operations. The first is that, because these operations are so important to the Russian military – they are deeply ingrained in its doctrinal logic – that they will doubtless be invested in and improved in the coming years. Lessons must have been learnt from experience in Ukraine. The likes of the GRU and other agencies will have understood, what works and what does not; where Ukrainian cyber defences are strong and where they might be weak. As a consequence, these Russian cyber agencies can also probably extrapolate and go on to establish where NATO cyber defences might also be strong and where weaknesses might lie.

It should be expected that, in the coming years, NATO states will experience more refined 'softening up' cyber-psychological attacks from the Russian military quarter. Western governments, elections, and even whole populations will be subjected to increased attempted 'manipulation' activities to degrees not seen before. This may result, as anticipated in the Russian military literature on this subject, in a long-term weakening of western institutions (NATO, European Union [EU], etc.) and a general undermining of the ability of individual NATO states to govern themselves effectively. Political vacuums could be created that might allow Moscow-leaning administrations to come to power. It should also be expected that cyber-technical attacks will continue against NATO states. These, though, will largely be confined to cyber-espionage activity seeking out weaknesses that can be exploited later and when necessary.

And then there is AI. AI will come to play a major part in the refining of future Russian IW activities. As its capabilities increasingly come to be utilised, AI will elevate the potency of all aspects of Russian cyberspace operations [83]. Cyber-psychological offensives that make use of social media can, with the application of AI, come to be far more targeted and more effective than hitherto. And AI-enhanced deepfakes of 'elite decision-makers' may become indistinguishable from the 'real' person and hence totally believable [84]. Cyber-technical attacks, enhanced by AI, could potentially be of an unimagined scale and impossible to counter.

But it is, of course, at times of very high geopolitical tension, or maybe even as preparation for major kinetic conflict with NATO, that Russian cyberspace operations may provide the greatest threat to NATO states. At such a time, a host of attacks – in combination and coordinated – using both cyber-psychological and cyber-technical means can be expected – from highly believable deepfakes to attacks that cripple a range of CNI targets (probably using previously planted malware). NATO states may then be unable to function as states. And if the state cannot function, then how can its military organisations? How then can NATO 'win' in a major kinetic conflict with Russia? And it may all be down to *mere* information.

References

[1] R. Morgus, B. Fonseca, K. Green, A. Crowther. (2019). *Are China and Russia on the cyber offensive in Latin America and the Caribbean?: A review of their cyber capabilities and implications for the US and its partners in the region*. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean [Accessed: Nov. 27, 2023].

[2] R. Thornton, M. Miron. (2022). Winning future wars: Russian offensive cyber and its vital importance in Moscow's strategic thinking, *Cyber Defense Review*, Summer, pp. 117–125. [Online]. Available: https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/09_Thorton_Miron_CDR_V7N3_Summer_2022.pdf?ver=0LhzDv4-cUkzkAqiTz401g%3D%3D [Accessed: Dec. 15, 2023].

[3] A. Polyakova. (Nov. 15, 2018). Weapons of the weak: Russia and AI-driven asymmetric warfare, *Brookings*. [Online]. Available: https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/. [Accessed: Dec. 11, 2023].

[4] J. Jashibekova. (Mar. 24, 2011). *Igor' Panarin: V informatsionnykh Voynakh u Rossii Dolzhen Byt' krepkii shchit IO.* [Online]. Available: https://aif.ru/society/igor_panarin_v_informacionnyh_voynah_u_rossii_dolzhen_byt_krepkiy_schit_i_o. [Accessed: Jan. 9, 2024].

[5] M.J. Mazarr, B. Frederick, Y.K. Crane. (2022). *Understanding a new era of strategic competition.* Santa Monica, CA: RAND. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA290-4/RAND_RRA290-4.pdf. [Accessed: Dec. 15, 2023].

[6] S. Duguin, P. Pavlova. (Sep. 2023). *The role of cyber in the Russian war against Ukraine: Its Impact and the consequences for the future of armed conflict.* [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf. [Accessed: Nov. 27, 2023].

[7] V. Medinsky. “Ivan Groznyi I informatsionnaya Voyna”, *Pravmir*, 06 Oct. 2016. [Online]. Available: https://www.pravmir.ru/ivan-groznyiy-i-informatsionnaya-voyna-video. [Accessed: Jan. 9, 2024].

[8] E. Messner. *Myatezh – Imya tretei mirovoi voyny.* Moscow: Moscow Publishing House, 1960.

[9] Kommersant, “Who is Igor Panarin,” Apr. 25, 2006. [Online]. Available: https://www.kommersant.ru/doc/669611. [Accessed: Dec. 11, 2023].

[10] J. Darczewska, “The anatomy of Russian information warfare. The Crimean operation, a case study,” *OSW Point of View*, no. 42, 2014. [Online]. Available: https://aei.pitt.edu/57173/1/42.pdf. [Accessed: Dec. 15, 2023].

[11] I. Panarin, *Pervaya mirovaya informatsionnaya voyna: Razval SSSR.* Saint Petersburg: Piter, 2010.

[12] V.V. Selivanov, Y.D. Il’yin, “Kontseptsiya voennotekhnicheskogo asimmetrichnogo otveta po sderzhivaniyu veroyatnogo protivnika ot razvyazyvaniya voennykh konflikov,” *Voennaya Mysl*, no. 2, pp. 31–47, 2022.

[13] I. Fazletdinov, V.I. Lumpov, “Rol’ Raketnykh voisk strategicheskogo naznacheniya v protivodeystvii strategicheskoi mnogosfernoi operatsii NATO,” *Voennaya Mysl*, no. 3, pp. 53–56, 2023.

[14] A. Mitrofanov, “Zakat yadernoi triady. Oruzhie SShA dlya naneseniya obezglavlivayushshego udara,” *Voennoe Obozrenie*, 15 Jan. 2020. [Online]. Available: https://topwar.ru/166706-zakat-jadernoj-triady-oruzhie-ssha-dlja-nanesenija-obezglavlivajuschego-udara.html. [Accessed: Nov. 27, 2023].

[15] J. Foreman, “Russia will not attack NATO,” *The Spectator*, 09 Mar. 2024. [Online]. Available: https://www.spectator.co.uk/article/russia-will-not-attack-nato/. [Accessed: Jan. 9, 2024].

[16] G. Austin, N. Khaniejo, “Impact of the Russia–Ukraine war on national cyber planning: A survey of ten countries,” *The International Institute for Strategic Studies*, Dec. 2024. [Online]. Available: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/01/impact-of-the-russiaukraine-war-on-national-cyber-planning_a-survey-of-ten-countries.pdf. [Accessed: Dec. 15, 2023].

[17] A.V. Il’nitsky, “Mental’naya Voyna Rossii,” *Voennaya Mysl*, no. 8, pp. 19–33, 2021.

[18] RBC. (Mar. 20, 2024). *Sovetnik shoygu zayavil o razrabotke NATO kognitivno-mental’nykh tekhnologiy*. [Online]. Available: https://www.rbc.ru/politics/20/03/2024/65fa3ad79a7947f594c076d6. [Accessed: Dec. 11, 2023].

[19] RIA Novosti. (Feb. 22, 2017). *Baluyevsky: Pobeda v informatsionnoi voine vazhnee, chem v klassicheskoi*. [Online]. Available: https://ria.ru/20170222/1488611839.html. [Accessed: Nov. 27, 2023].

[20] V. Gerasimov, “Tsennost’ Nauki v Predvidenii,” *Voenno- Promyshlenyi Kur’er*, 27 Feb. 2013. [Online]. Available: http://www.vpk-news.ru/articles/14632. [Accessed: Nov. 27, 2023].

[21] S.G. Chekinov, S.A. Bogdanov, “Vliyaniye asimmetricheskikh deystviy na sovremennuyu bezopasnost’ Rossii,” *Vestnik Akademii Voennykh Nauk*, no. 1, pp. 46–53, 2010.

[22] S.A. Bogdanov, S.G. Chekinov, “Asimmetrichnye deistviya po obespecheniyu voennoi bezopasnosti Rossii,” *Voennaya Mysl*, no. 3, pp. 13–22, 2010.

[23] A. Barthosh. (Aug. 12, 2021). *Gibridnaya, skrytnaya, nepredskazuyemaya, Nezavisimoye Voennoye Obozreniye*. [Online]. Available: https://nvo.ng.ru/gpolit/2021-08-12/1_10_11_1153_hybrid.html. [Accessed: Dec. 15, 2023].

[24] A. Barthosh, “Informatsionno-psikhologicheskaya bor’ba obretaet novye sredstva,” *Nezavisimoye Voennoe Obozreniye*, 28 Sep. 2023. [Online]. Available: https://nvo.ng.ru/concepts/2023-09-28/1_1255_propaganda.html. [Accessed: Nov. 27, 2023].

[25] S.P. Rastorguev. (1999). Informatsionnaya voyna: Problemy I modeli. Moscow: Radio and Communication. [Online]. Available: https://community.apan.org › __key › docpreview-s. [Accessed: Nov. 27, 2023].

[26] B. DeWees, T.C. Pierce, E.J. Rokke, A. Tingle, “Toward a unified metric of kinetic and nonkinetic actions,” *Joint Force Quarterly*, no. 85, 2017. [Online]. Available: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_16-21_DeWees-et-al.pdf. [Accessed: Dec. 11, 2023].

[27] President of the Russian Federation. (Dec. 31, 2015). *Strategiya natsional’noi bezopasnosti Rossiiskoi federatsii,* Moscow: The Kremlin. [Online]. Available: https://rg.ru/documents/2015/12/31/nac-bezopasnost-site-dok.html. [Accessed: Dec. 15, 2023].

[28] I. Panarin, Informatsionnaya voyna i geopolitika [Information war and geopolitics], Moscow: Pokolenie, 2006.

[29] V.M. Burenok, E.V. Gorgola, S.F. Vykulov. (2015). *Natsional’naya bezopasnost’ Rossii v epokhy setevykh voin*, Moscow: Granitsa. [Online]. Available: https://sc.mil.ru/files/morf/military/archive/VIE-41.pdf. [Accessed: Nov. 27, 2023].

[30] V.V. Izonov, “On the issue of political mechanisms to counter external threats to Russia’ military security,” *Nauka, Obshestvo, Oborona*, vol. 6, no. 1, 2016. [Online]. Available: https://www.noo-journal.ru/nauka-obshestvo-oborona/2016-1-6/article-0059/. [Accessed: Dec. 11, 2023].

[31] A.V. Manoilo, “Informatsyonno-psikhologicheskaya voyna: Faktory, opredelayushchiye format sovremennogo vooruzhennogo konflikta.” Materials of the V International Scientific and Practical Conference on Information Technologies and Security, no. 8, Kyiv, 2005, pp. 73–80.

[32] S.P. Rastorguev, M.V. Litvinenko, *Informatsionnye operatsii v seti internet*. Moscow: ANO Tsentr Strategicheskikh Otsenok I Prognozov, 2014.

[33] A. Khramchikhin, “Novyi Sposob Vedeniya Voyn,” *Voenno-Promyshlennyi Kur’er*, 17 Feb. 2020. [Online]. Available: https://vpk.name/news/375164_novyi_sposob_vedeniya_boya.html. [Accessed: Dec. 15, 2023].

[34] S. Shandler, M.L. Gross, D. Canetti, “Cyberattacks, psychological distress, and military escalation: An internal meta-analysis,” *Journal of Global Security Studies*, vol. 8, no. 1, pp. 1–19, 2023, doi: 10.1093/jogss/ogac042.

[35] A. Greenberg, “Hackers hit Macron with huge email leak ahead of French elections,” *Wired*, 05 May 2017. [Online]. Available: https://www.wired.com/2017/05/macron-email-hack-french-election/. [Accessed: Nov. 27, 2023].

[36] D.V. Gioe, “Cyber operations and useful fools: The approach of Russian hybrid intelligence,” *Intelligence and National Security*, vol. 33, no. 7, pp. 954–973, 2018, doi: 10.1080/02684527.2018.1479345.

[37] H. Tanriverdi, F. Flade, L. Frey. (Feb. 17, 2022). *The elite hackers of the FSB*. [Online]. Available: https://interaktiv.br.de/elite-hacker-fsb/en/index.html. [Accessed: Dec. 11, 2023].

[38] A. Soldatov, I. Borogan, "Kibersily Rossii: Kak eto rabotayet," *Agentura.ru*, 2022. [Online]. Available: https://agentura.ru/investigations/kibersily-rossii-kak-jeto-rabotaet/. [Accessed: Jan. 16, 2024].

[39] A. Scarsi, "Prigozhin's corporate network 'aims at destabilising' the west with 'information warfare'," *Daily Express,* 26 Jul. 2023. [Online]. Available: https://www.express.co.uk/news/world/1795164/Yevgeny-Prigozhin-threat-western-democracies-information-warfare. [Accessed: Dec. 15, 2023].

[40] M. Simonyan, "Simonyan: Informatsiya kak oruzhye ispol'zuyetsya temi, kto imeet vozmozhnost'," *Rossiyskaya Gazeta,* 03 Jul. 2013. [Online]. Available: https://rg.ru/2013/07/03/simonian.html. [Accessed: Jan. 9, 2024].

[41] J. Hakala, J. Melnychuk. (2021). *Russia's strategy in cyberspace*, NATO Strategic Communications Centre of Excellence. [Online]. Available: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf. [Accessed: Nov. 27, 2023].

[42] A.S. Bowen, "Russian cyber units," *Congressional Research Service*, 02 Feb. 2022. [Online]. Available: https://sgp.fas.org/crs/row/IF11718.pdf. [Accessed: Dec. 11, 2023].

[43] H. Warrell, M. Seddon, K. Manson, "Russia military unit accused of Georgia cyber attacks," *Financial Times*, 24 Feb. 2020. [Online]. Available: https://www.ft.com/content/14377b84-53e3-11ea-90ad-25e377c0ee1f. [Accessed: Dec. 15, 2023].

[44] A. Troianovski, E. Nakashima, "Russia's military intelligence agency became the covert muscle in Putin's duels with the west," *The Washington Post*, 27 Dec. 2018. [Online]. Available: https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html. [Accessed: Nov. 27, 2023].

[45] M. Roache, S. Tewa, A. Cadier, Ch. Labbe, V. Padovese, et al., "Russia-Ukraine disinformation tracking center: 470 websites spreading war disinformation and the top myths they publish," *Newsguard*, 24 May 2024. [Online]. Available: https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/. [Accessed: Dec. 11, 2023].

[46] A. Greenberg, *Sandworm: A new era of cyberwar and the hunt for Kremlin's most dangerous hackers.* New York, NY: DoubleDay, 2020.

[47] A. Greenberg, "This Is the new leader of Russia's infamous sandworm hacking unit," *Wired*, 15 Mar. 2023. [Online]. Available: https://www.wired.com/story/russia-gru-sandworm-serebriakov/. [Accessed: Dec. 11, 2023].

[48] J. Hultquist, "Sandworm team and the Ukrainian power authority attacks," *Mandiant*, 07 Jan. 2016. [Online]. Available: https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team. [Accessed: Jan. 16, 2024].

[49] United States Department of Justice. (Oct. 19, 2022). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace.* [Online]. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. [Accessed: Jan. 9, 2024].

[50] D.E. Sanger, N. Perlroth, "Russian intelligence hackers are back, microsoft warns, aiming at officials of both parties," *The New York Times*, 10 Sep. 2020. [Online]. Available: https://www.nytimes.com/2020/09/10/us/politics/russian-hacking-microsoft-biden-trump.html. [Accessed: Dec. 11, 2023].

[51] J. Przetacznik, S. Tarpova. (Jun. 08, 2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549. [Accessed: Dec. 15, 2023].

[52] M. Burgess, "A mysterious satellite hack has victims far beyond Ukraine," *Wired*, 23 Mar. 2022. [Online]. Available: https://www.wired.com/story/viasat-internet-hack-ukraine-russia. [Accessed: Jan. 9, 2024].

[53] C. Albon, "Experts say Russia's use of counterspace capabilities could make 2022 a 'pivotal' year for space security," *Defense News*, 04 Apr. 2022. [Online]. Available: https://www.defensenews.com/battlefield-tech/space/2022/04/04/experts-say-russias-use-of-counterspace-capabilities-could-make-2022-a-pivotal-year-for-space-security/. [Accessed: Nov. 27, 2023].

[54] A.J. Vicens, "UK, EU, US formally blame Russia for Viasat satellite hack before Ukraine invasion," *Cyberscoop*, 10 May 2022. [Online]. Available: https://cyberscoop.com/viasat-hack-russia-uk-eu-us-ukraine/. [Accessed: Dec. 11, 2023].

[55] V. Zhora. (May 18, 2022). *How to ride a bear – Russian cyber posture and security implications*, CyberSec Forum/Expo, Katowice, Poland. [Online]. Available: https://www.youtube.com/watch?v=lI7PQP_IcdA. [Accessed: Dec. 15, 2023].

[56] J. Bateman. (Dec. 16, 2022). *Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications*, Carnegie Endowment for International Peace, Washington, DC, Paper. Available: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en&center=global [Accessed: Jan. 16, 2024].

[57] L. Collins, M. Kofman, J. Spencer, "The battle of Hostomel airport: A key moment in Russia's defeat in Kyiv," *War on the Rocks*, 10 Aug. 2023. [Online]. Available: https://warontherocks.com/2023/08/the-battle-of-hostomel-airport-a-key-moment-in-russias-defeat-in-kyiv/. [Accessed: Dec. 11, 2023].

[58] A. Molchanova, "V Provedenii IPsO Protiv Ukrainy Zadeystvovany GRU, FSB I Prigozhinskiye Trolli – Kak Oni Deistvuyut. Intervyu s Polkovnikom VSU," *Obozrevatel*, 14 Dec. 2022. [Online]. Available: https://war.obozrevatel.com/polkovnik-vsu-taras-dzyuba-ipso-kak-rossiya-provodit-informatsionnyie-operatsii-protiv-ukrainyi.htm. [Accessed: Jan. 16, 2024].

[59] T. Simonite, "A Zelensky deepfake was quickly defeated. The next one might not be," *Wired*, 17 Mar. 2022. [Online]. Available: https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/. [Accessed: Nov. 27, 2023].

[60] D. Black, G. Roncone, "The GRU's disruptive playbook," *Mandiant*, 12 Jul. 2023. [Online]. Available: https://www.mandiant.com/resources/blog/gru-disruptive-playbook. [Accessed: Dec. 11, 2023].

[61] K. Proska, J. Wolfram, J. Wilson, D. Black, K. Lunden, et al., "Sandworm disrupts power in Ukraine using a novel attack against operational technology," *Mandiant*, 09 Nov. 2023. [Online]. Available: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology. [Accessed: Jan. 9, 2024].

[62] A. Greenberg, “Sandworm hackers caused another blackout in Ukraine–During a missile strikes,” *Wired*, 09 Nov. 2023. [Online]. Available: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/. [Accessed: Jan. 16, 2024].

[63] J. Pearson, “Russian spies behind cyber attack on Ukraine power grid in 2022 – Researchers,” *Reuters*, 11 Nov. 2023. [Online]. Available: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/. [Accessed: Dec. 15, 2023].

[64] P. Muncaster, “Microsoft warns of destructive malware campaign targeting Ukraine,” *Infosecurity Magazine*, 17 Jan. 2022. [Online]. Available: https://www.infosecurity-magazine.com/news/microsoft-destructive-malware/. [Accessed: Dec. 11, 2023].

[65] Microsoft Threat Intelligence. (Jun. 14, 2023). *Cadet Blizzard emerges as a novel and distinct Russian threat actor.* [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/. [Accessed: Nov. 27, 2023].

[66] A.J. Vincens, “Microsoft identifies new hacking unit within Russia’s military intelligence,” *Cyberscoop*, 14 Jun. 2023, [Online]. Available: https://cyberscoop.com/microsoft-gru-russia-ukraine-hacking/. [Accessed: Dec. 15, 2023].

[67] K. Giles, “Russian cyber and information warfare in practice,” *Chatham House*, 14 Dec. 2023. [Online]. Available: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice. [Accessed: Jan. 9, 2024].

[68] RBC. (Nov. 1, 2023). *Glava minzyfry podderzhal sozdaniye kibervoisk*. [Online]. Available: https://www.rbc.ru/rbcfreenews/654224319a79471580f33da6. [Accessed: Jan. 16, 2024].

[69] V. Kiselev, A. Kostenko, “Kibervoyna kak Osnova Gibridnoi Operatsii,” *Armeiskii Sbornik*, vol. 11, no. 257, pp. 3–6, 2015. [Online]. Available: https://sc.mil.ru/files/morf/military/archive/AS_11_2015.pdf. [Accessed: Dec. 11, 2023].

[70] P.I. Antonovich, “O sushhnosti I soderzhanii kibervoyny,” *Voennaya Mysl*, no. 7, pp. 39–46, 2011.

[71] R. Hastings, “Why Russia’s cyber warfare has failed in Ukraine – But remains a threat to the UK,” *I News*, 16 Jun. 2023. [Online]. Available: https://inews.co.uk/news/technology/russia-cyber-warfare-failed-ukraine-threat-uk-2404924. [Accessed: Dec. 15, 2023].

[72] D. Vergun, “Partnering with Ukraine on cybersecurity paid off, leaders say,” *DOD News*, 03 Dec. 2022. [Online]. Available: https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/. [Accessed: Dec. 11, 2023].

[73] M. Kofman, R. Connolly, J. Edmonds, A. Kendall-Taylor, S. Bendett, “Assessing Russian state capacity to develop and deploy advanced military technology,” *Center for a New American Security*, 21 Oct. 2022. [Online]. Available: https://www.cnas.org/publications/reports/assessing-russian-state-capacity-to-develop-and-deploy-advanced-military-technology. [Accessed: Nov. 27, 2023].

[74] N. Eftimiades, “Small satellites: The implications for national security,” *Atlantic Council*, 05 May 2022. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/small-satellites-the-implications-for-national-security/. [Accessed: Jan. 9, 2024].

[75] J. Pavur, I. Martinovich, “The cyber-ASAT: On the impact of cyber weapons in outer space,” *IEEE Xplore*, May 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8756904. [Accessed: Jan. 16, 2024].

[76] D.T. Burbach, “Early lessons from the Russia-Ukraine war as a space conflict,” *Atlantic Council*, 30 Aug. 2022. [Online]. Available: https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/. [Accessed: Dec. 11, 2023].

[77] J. Menn, “Cyberattack knocks out satellite communications for Russian military,” *Washington Post*, 30 Jun. 2023. [Online]. Available: https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/. [Accessed: Jan. 9, 2024].

[78] E. Howell, “Elon Musk says Russia is ramping up cyberattacks on SpaceX’s Starlink systems in Ukraine,” *Space*, 14 Oct. 2022. [Online]. Available: https://www.space.com/starlink-russian-cyberattacks-ramp-up-efforts-elon-musk. [Accessed: Nov. 27, 2023].

[79] European Space Policy Institute. (Oct. 10, 2022). *The war in Ukraine from a space cybersecurity perspective*. [Online]. Available: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf. [Accessed: Dec. 11, 2023].

[80] D. Goward, “Why isn’t Russia doing more to jam GPS in Ukraine?”, *C4ISRNET*, 22 Jul. 2022. [Online]. Available: https://www.c4isrnet.com/opinion/2022/07/22/why-isnt-russia-jamming-gps-harder-in-ukraine/. [Accessed: Dec. 15, 2023].

[81] R. Thomas, “Russian aggression shows the west’s GNSS weakness,” *Army Technology*, 19 Aug. 2022. [Online]. Available: https://www.army-technology.com/interviews/russian-aggression-shows-the-wests-gnss-weakness/. [Accessed: Jan. 9, 2024].

[82] A.R. Sarkar, “China building cyber weapons to ‘seize control’ of enemy satellites, says leaked CIA report,” *The Independent*, 21 Apr. 2023. [Online]. Available: https://www.independent.co.uk/asia/china/cyber-weapon-satellite-cia-report-b2324222.html. [Accessed: Nov. 27, 2023].

[83] R. Thornton, M. Miron, “Towards the ‘third revolution in military affairs’: The Russian military’s use of AI-enhanced cyber warfare,” *RUSI Journal*, vol. 165, no. 3, pp. 12-21, 2020, doi: 10.1080/03071847.2020.1765514 [Online]. Available: https://rusi.org/publication/rusi-journal/towards-%E2%80%98third-revolution-military-affairs%E2%80%99-russian-military%E2%80%99s-use-ai. [Accessed: Jan. 16, 2024].

[84] L. Hay Newman, “AI-generated voice deepfakes aren’t scary good – Yet,” *Wired*, 15 Mar. 2023. [Online]. Available: https://www.wired.com/story/ai-voice-deepfakes/. [Accessed: Jan. 9, 2024].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Investment in Cybersecurity Companies in Times of Political and Economic Instability

Grzegorz Przekota | Koszalin University of Technology, Poland |
ORCID: 0000-0002-9173-2658

Received: 18.03.2024

Accepted: 01.06.2024

Published: 18.07.2024

Cite this article as:
G. Przekota "Investment in cybersecurity companies in times of political and economic instability," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190342

Corresponding author:
Grzegorz Przekota, Koszalin University of Technology, Poland.
E-mail: grzegorz.przekota@tu.koszalin.pl;
0000-0002-9173-2658

Abstract

The socio-economic development that has taken place in recent years takes into account cybersecurity issues. Cybersecurity has many different dimensions, including the economic dimension. The Russian-Ukrainian conflict has shown that modern war is not only conventional, but also cybernetic. Earlier, the massive shift to remote communication systems forced by COVID also increased the demand for cybersecurity. This means that cybersecurity companies receive new orders, which can have a positive impact on their financial results. In the opinion of many experts, investing in such companies could be a good business. The research conducted in this article focuses on testing assumptions related to the recognition of investments in technology companies as prospective investments. Therefore, this study examines the impact of Russia-Ukraine war (from February 2022 to December 2024) and the COVID pandemic (from March 2020 to February 2022) on the valuation of cybersecurity companies. The period from January 2015 to February 2020 was used as the comparative period. The research material consists of companies and stock indices from the American and Polish markets. The results of the research are inconclusive. In fact, there are some examples of companies that took advantage of the Russian-Ukrainian conflict to achieve above-average returns. Such a business is risky, which is why these companies are achieving above-average returns with increased shares price volatility. However, it turns out that automatically assigning a company to the cyber or IT category does not mean that it will be a good investment in times of war or pandemic.

Keywords

cybersecurity threat, enterprise development, investments, stock exchange

1. Introduction

In recent years, the importance of concepts such as the computerisation of the economy, modern technologies, the Internet of things, information security, and cybersecurity has been particularly emphasised [1]. They are related to modern production processes that are increasingly computerised, in the provision of both material goods and services.

The last few years in the Eastern European region have been years of anxiety related to the Russian-Ukrainian conflict. This is an event that directly or indirectly has affected all European countries and a significant number of non-European countries. The war has affected the world not only in the physical dimension but also in the cyberspace dimension. Modern conflicts are not only conducted in a conventional way but also in a hybrid way, and the parties to the conflict make extensive use of the cyber world. Governments, companies, and individuals are being attacked through information technology (IT) networks. Cyberattacks have prompted decision-makers and companies to take active steps to limit the impact of cyberattacks. On the one hand, society is being made aware of media manipulation, which is most easily carried out via Internet media, and on the other hand, systems and software are being built to protect against cyberattacks. This is where business issues come into play. On the one hand, war results in significant human and material losses, on the other hand, it is a profitable industry for both arms and IT sectors.

External threats that negatively impact cybersecurity have quickly become an extreme risk and threat to global development [2]. Addressing this challenge from a global perspective requires appropriate and focused resolve [3].

Cybersecurity is associated with technical security measures and solutions, such as encryption, intrusion prevention systems, and access control to IT systems. The business aspects of cybersecurity have been growing for at least 40 years [4]. In his reflections at the time, Courtney stated that the decision whether to protect against

IT attacks requires weighing all the costs and benefits, and that security controls should not be implemented if they cost more than tolerating the problem. This approach is related to the neoclassical approach to economic problems, which is dominated by rationality and optimisation of behaviour [5]. Reality, however, is more stochastic and uncertain, and information is not perfect.

A World Economic Forum report identified cybersecurity failures as a clear and present threat. The scale of cybersecurity threat is difficult to estimate [6]. Different sources come up with different calculations. According to data, by 2020, the cost of cybercrime was estimated at $1 trillion and investments in cybersecurity stood at $145 billion [7], with these values growing rapidly from year to year [8]. The difficulty in estimating the cost of cybercrime is primarily due to the complexity of the problem, while economic models simplify reality. Therefore, all research that addresses the issue of cybercrime and cybersecurity develops the perception of the problem and shows the extent of its impact, both direct and indirect.

Cybersecurity is a very broad concept. It is defined differently in the literature on the subject. From the point of view of this study, it can be assumed that cybersecurity includes various procedures that create a secure environment by protecting assets, and an asset is anything that has a certain value [9]. Assets are those things that require special protection against illegal access, use, disclosure, modification, destruction, and/or theft that could result in loss to the organisation. Because assets are of different types, the scope of cybercrime is very broad, ranging from the theft of data or the disclosure of confidential or compromising information to attacks on physical assets.

A broad economic view of cybersecurity is proposed by Rathod and Hämäläinen, who formulate public policy recommendations aimed at adapting policies and regulations to ensure trust in the digital environment, and also postulate a combination of economic and cybersecurity analysis that provides reference points for the economic assessment of national and international cybersecurity audits and standards [10]. Meanwhile, Ahmed notes that cybercrime costs companies and countries significant amounts of money and disrupts economic and financial activities around the world [11]. Estimates of the financial and physical costs associated with cybercrime motivate investment in cybersecurity. While it is the responsibility of governments to ensure that laws are in place to combat cybercrime, all organisations need to take protective measures commensurate with the threat. This is where companies that develop and supply software to protect organisations' assets come into play. This is undoubtedly a developing industry. For example, in Poland, the participation of Section J (Information and Communication) in gross domestic product (GDP), which includes Section 62 – Activities related to software and IT consultancy and related activities – was at a record high of 4.92% of GDP in 2022, increasing by more than 1 percentage point over the last decade [12].

There are reports and publications on news websites and specialised websites that suggest that investing in cybersecurity companies is currently one of the best forms of investing capital (see, Websites). Such studies are an important part of financial markets because they influence investor's opinion.

Organisations defend themselves against cyber threats in a variety of ways. There is some debate in the literature about how the level of security depends on the design of the system, whether the defence depends on the efforts of the laziest defender, the bravest defender, or the sum of all defenders [13]. Basically, it corrects the idea that a software company should hire fewer but better programmers, more testers, and the best security architect it can find [14]. From the point of view of investors in a company's shares, it is extremely difficult to assess, but this can be done indirectly by assessing the market success of the software that the company sells.

Based on the suggestion that investing in cybersecurity companies is a profitable business, following are the three objectives for this study:

1. To test whether software companies, especially those that provide protection against cyber threats, perform better than stock market indices that reflect the overall market situation.
2. To check whether the situation regarding investments in cyber companies in Poland, which is nearer to the Russian-Ukrainian conflict, is different from that in the United States.
3. To examine the impact of the war, compared to the impact of the COVID pandemic.

These are three issues that helped to test the recommendations for investing in technology companies.

2. Methods

The research focused on the rates of return for four American and four Polish companies. The choice of companies was deliberate. In the case of the American companies, they are the largest cybersecurity companies listed on the NASDAQ stock exchange, including the following:

1. Cisco Systems (CSCO.US)
2. Palo Alto Networks Inc (PANW.US)
3. Fortinet (FTNT.US)
4. Check Point Software Technologies Ltd (CHKP.US)

These companies were evaluated against the NASDAQ index.

In the case of the Polish Stock Exchange, these companies are involved in the development and supply of software. The condition for participation in the study was that the company had been operating as a listed company for at least 9 years, including the following:

1. Asseco Poland SA (ACP)
2. Comarch SA (CMR)
3. Sygnity SA (SGN)
4. LSI Software SA (LSI)

These companies were evaluated against the Warsaw Stock Exchange General (WIG) index.

The period of the research covers the years 2015–2023 and is divided into the following three sub-periods:

1. January 2015–February 2020
2. March 2020–February 2022
3. February 2022–December 2023

Weekly frequency data was examined.

The division of periods coincided with the COVID pandemic and beginning of Russia’s military operations in Ukraine, and the interest lies in determining the difference in the statistics of the companies’ quotations against the relevant stock market indices during pandemic and after the start of hostilities, compared to the previous period.

The research is divided into two stages:

1. Price formation of share stock in relation to stock market indices. The data is presented in logarithmic form. This method

makes it easy to assess the rate of increase in the value of the quotations, as small differences can be seen:

$$\ln y_{t+1} - \ln y_t = \ln \frac{y_t + 1}{y_t} \approx \frac{y_{t+1}}{y_t} = -1$$

The graph uses a main unit of 0.5, which represents an increase in the value of the quotes of approximately 65%, regardless of the level. Separate graphs show the relative increases in price. These graphs show the strength of the changes and highlight periods of above-average change.

2. Overview of the descriptive statistics of the return rate series:
   - Mean – average of weekly returns interpreted as average weekly income;
   - St. Dev. – standard deviation of weekly returns, allowing the assessment of the absolute strength of diversification of returns, interpreted as total risk.

The research is supplemented by graphical representation of the company's return and risk on a risk-return graph in three time intervals.

3. Results

Figure 1 shows the share prices of the US-listed companies against the backdrop of the NASDAQ index. The NASDAQ index was in an upward trend until the end of 2021. However, from the beginning of 2022, it entered a short downward phase that lasted for 1 year. In 2023, the NASDAQ index began to recover, but the growth rate was quite slow and 2023 ended at a lower level than the 2021 peak.

The American market is a very large market and the companies listed there tend to be global companies. Therefore, the start of military operations in Ukraine may have caused some pessimism among investors about the possibility of further positive developments. This uncertainty was reflected in index declines in 2022. What experts often emphasise is that societies have become accustomed to certain situations, including tragic ones. This habit and the adaptation of companies to the new situation led to this negative trend being replaced by a moderately positive trend from 2023.

Interesting is how the cybersecurity companies, for whom the threat of cyberattacks is the basis for building commercial strategies and protection against cyberattacks is the main source of revenue,

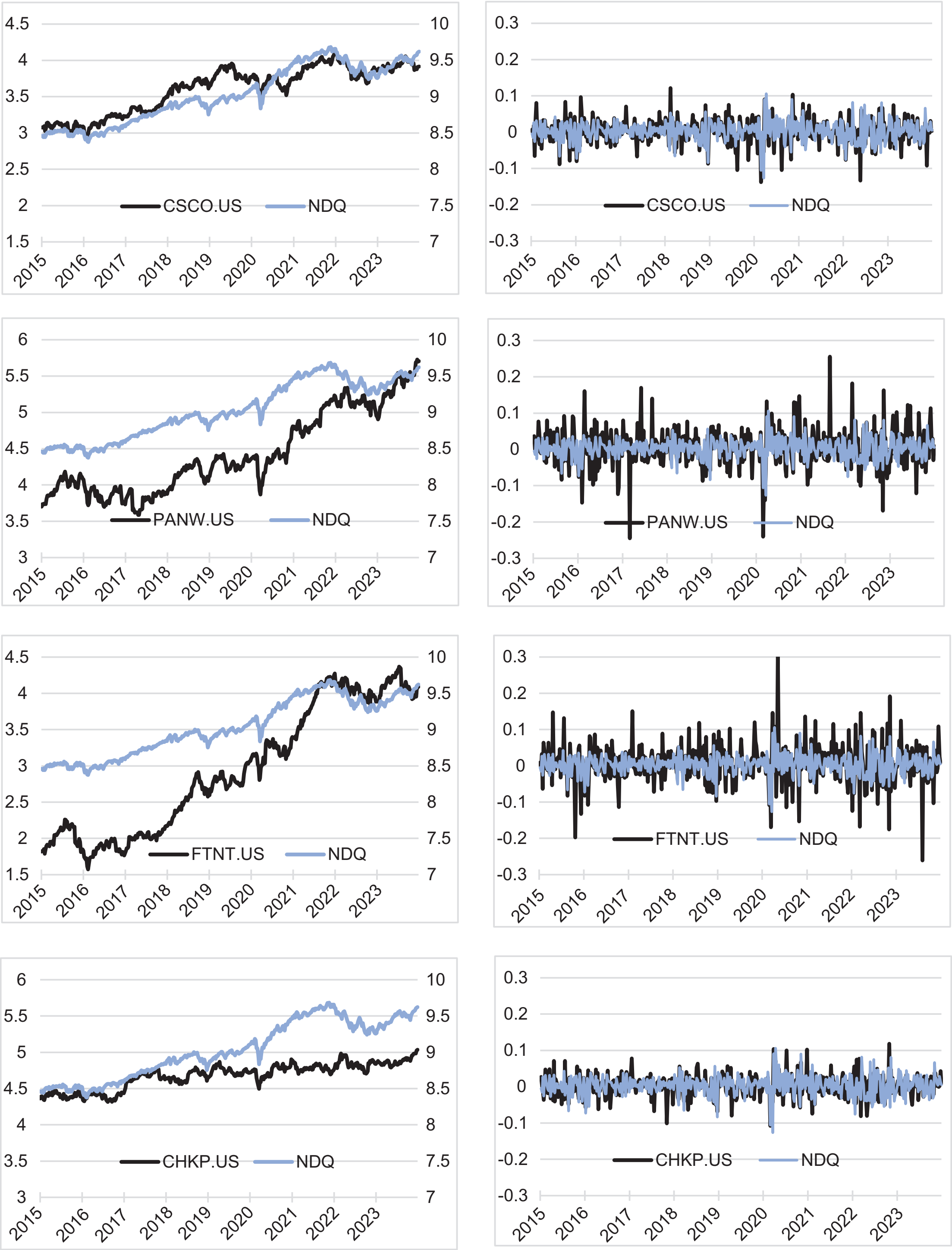


Figure 1. Share price performance of the US technology companies, 2015–2023.

have coped with this situation. It turns out that, in general, all the companies recorded an increase in value throughout the period, but the pace of this increase varied, with the highest being PANW and FTNT, and the clearly weaker being CSCO and CHKP. PANW and FTNT grew at a rate well above that of the NASDAQ index, the third at a similar rate to the NASDAQ and the last at a much slower rate. Therefore, the mere qualification as a modern technology company was not enough to achieve a good growth rate, which proves the rationality of investors who make decisions based on other information as well. It should be noted that all four companies are being promoted in the media as potentially good investments.

The COVID pandemic did not stop this growing trend, but rather strengthened it. The disruption was only temporary at the beginning of the pandemic announcement, but the short-term declines were significant; then there were increases.

What happened after the outbreak of hostilities in Ukraine is particularly interesting. In the period following the outbreak of war, PANW was the best performer, with a spectacular increase in value. The company is constantly monitoring the situation regarding cyberattacks related to the Russian-Ukrainian war [15].

The graphs on the right side show the rates of return. The most interesting concern is the volatility following Russia's invasion of Ukraine. There is a slightly larger increase in volatility. However, even in the period up to 2022, there are sub-periods with increased volatility, such as the pandemic period. In general, it is natural for any period of economic or political uncertainty to increase volatility in capital markets.

The situation on the Polish stock market was different (Figure 2). First, until the end of 2021, the WIG index was in a very weak upward trend. The year 2022, similar to the NASDAQ, was a year of decline, but the year 2023 brought a strong recovery in value, and the WIG index saw the end of 2023 with a record value.

The COVID pandemic initially caused a significant drop, but then WIG prices started to rise. However, companies behaved differently.

It is worth noting that Polish companies do not have the same influence as American companies. In terms of capitalisation, the Polish companies analysed are clearly inferior to their American counterparts. The fourth American company analysed by capitalisation,

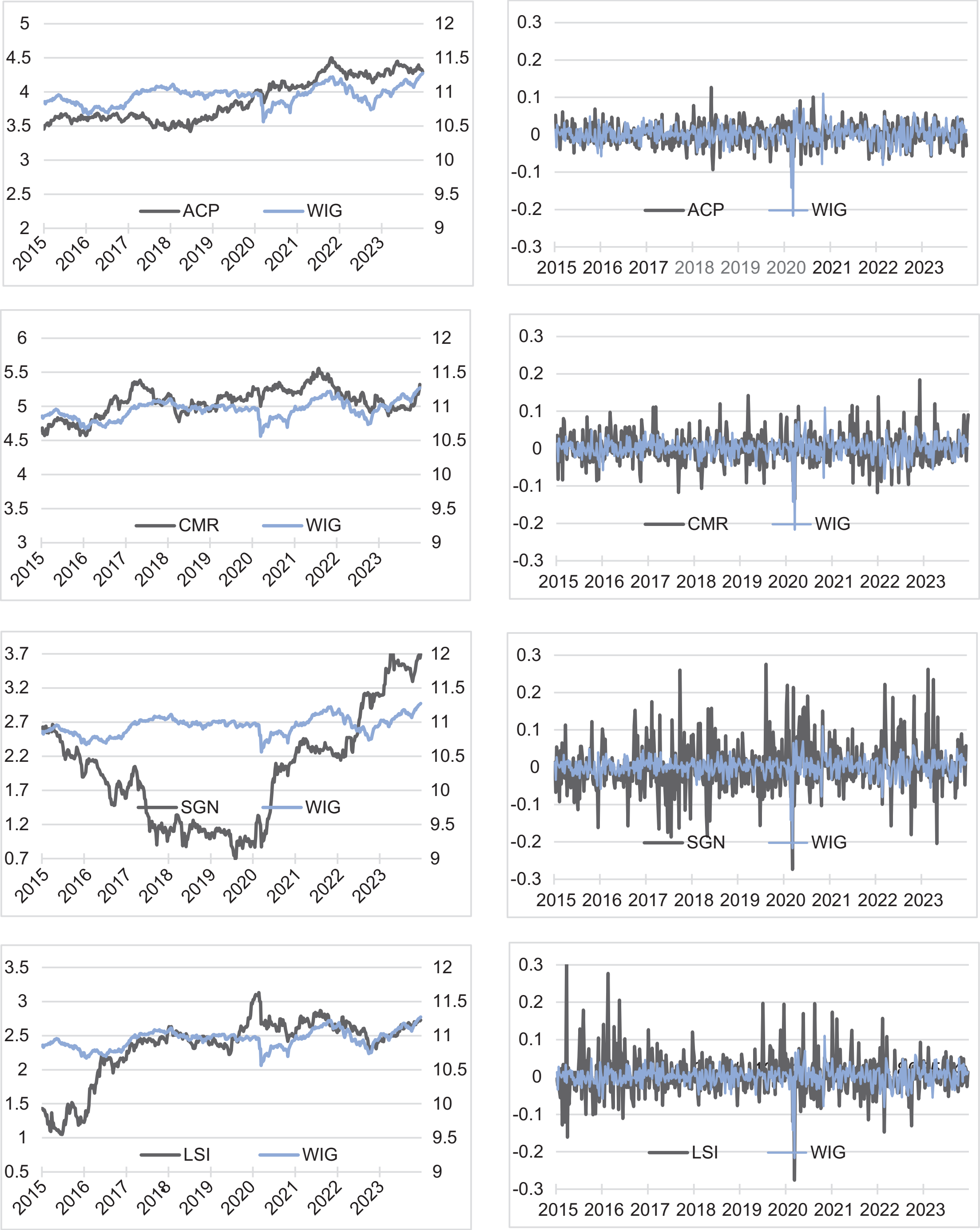


Figure 2. Share price performance of Polish technology companies, 2015–2023.

CHKP, has a capitalisation ten times higher than the largest Polish company analysed, ACP.

Taking into account the situation after Russia's aggression against Ukraine, the best Polish company is SGN, which intensively implements software in Ukraine as well.

The characteristics noted in the graphs are translated into rates of return descriptive statistics (Table 1). First of all, we observed that the range of average returns increases in the pandemic period and after Russia's invasion of Ukraine:

- For the American market:
    - Until March 2020 – the range was between 0.18% for CHKP and 0.59% for FTNT.
    - Between March 2020 and February 2022 – the range was between 0.17% for CHKP and 1.14% for FTNT.
    - From February 2022 – the range was between -0.05% for CSCO and 0.82% for PANW.
- For the Polish market:
    - Until March 2020 – the range was between -0.25% for SGN and 0.80% for LSI.
    - Between March 2020 and February 2022 – the range was between -0.13% for LSI and 1.17% for SGN.
    - From February 2022 – the range was between 0.03% for LSI and 1.75% for SGN.

Table 1. Descriptive statistics of time series of weekly returns.

Index/ company	01.2015–03.2020		03.2020–02.2022		02.2022–12.2023	
	Mean (%)	St. Dev.	Mean (%)	St. Dev.	Mean (%)	St. Dev.
NDQ	0.29	2.13	0.40	3.50	0.16	3.27
CSCO.US	0.30	3.11	0.33	3.68	-0.05	3.42
PANW.US	0.36	4.52	0.83	5.89	0.82	5.83
FTNT.US	0.59	4.37	1.14	6.33	0.19	6.41
CHKP.US	0.18	2.69	0.17	3.54	0.21	3.05
WIG	0.06	1.87	0.20	3.72	0.23	2.84
ACP	0.25	2.88	0.31	3.31	0.05	3.05
CMR	0.31	3.96	0.02	4.63	0.25	4.38
SGN	-0.25	6.80	1.17	6.87	1.75	7.59
LSI	0.80	5.80	-0.13	6.42	0.03	3.86

These results intend that the pandemic and the war have significantly widened the gap between companies' average weekly returns, compared to the previous period. Companies are therefore coping with political and economic instability in very different ways, with some being benefitted and others losing out.

For all US companies, the standard deviation increases after 2020 and 2022. Similarly for all Polish companies until 2020, and for three of the four Polish companies after 2022 (except LSI). The value of standard deviation for the whole stock market (standard deviation of the indices) also increases. Interestingly, however, the volatility measured by the standard deviation from February 2022 is lower for the Polish stock exchange, which is closer to the conflict, than for the American stock exchange.

In general, it would appear that modern IT companies achieve better financial results after the outbreak of hostilities and the increased number of cyberattacks, which is reflected in above-average increases in share prices. This assumption is also consistent with many of the articles cited above, which encourage investment in technology companies. However, the situation is more complicated. This is shown in Figure 3.

The COVID pandemic situation and the subsequent war in Ukraine have changed the stock market situation for cybersecurity companies. Every company behaves differently.

Taking into account the detailed objectives of the research, it can be said that technology companies in the period of economic and political stabilisation do not stand out from the stock market indices as companies with above-average returns. However, the economic destabilisation that took place during the COVID pandemic, or the political destabilisation that has taken place since the war in Ukraine, causes the results of the companies to become more uneven, with some performing better and others worse. The war and the pandemic have increased the overall volatility in both Poland and the United States. Capital markets are global markets, so stock market reactions are often similar, even if they are in different regions of the world.

Companies that have benefited from the COVID pandemic include FTNT and PANW in the United States and SGN in Poland. Of them, PANW from the United States and SGN from Poland increase in value during war. In general, the situation of PANW from the US market and SGN from the Polish market can be described as classic.

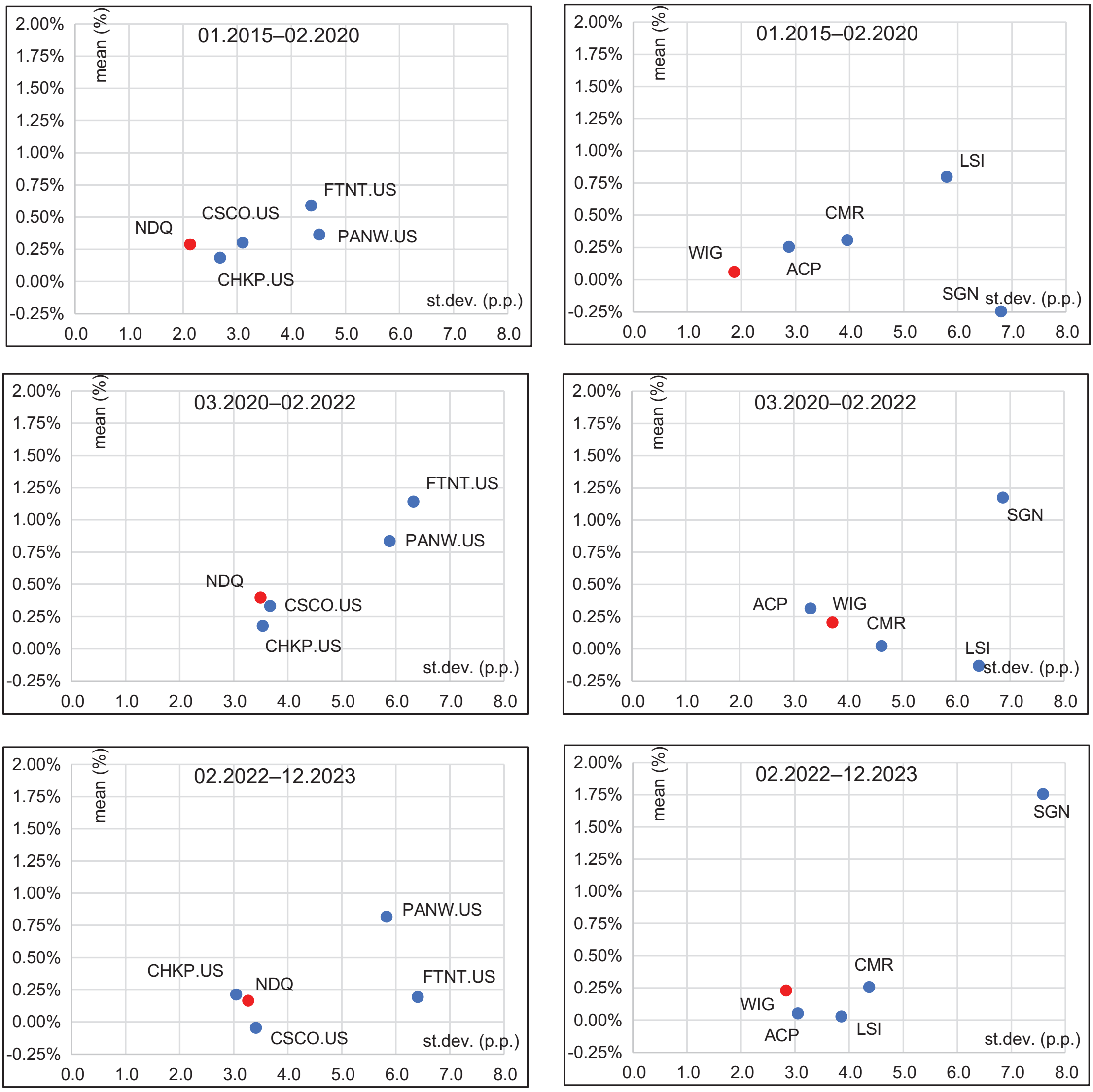


Figure 3. Risk-return map for technology companies in the United States and Poland.

On the charts, these companies are located in the upper right corner (03.2020–02.2022 and 02.2022–12.2023). The position of the risk-return map in the upper right corner of the chart means that such a company has achieved high returns with significant price volatility. This is a classic situation for companies involved in risky projects, such as cyber threats related to the Russian-Ukrainian conflict. The situation of other companies is very different. Some have lost their growth momentum after 2022, others have gained. Each company has its own specificities, and it is not possible here to generalise the same.

4. Conclusions

The war industry has always been seen as a harbinger of economic change. Countries that fought wars to gain a military advantage developed techniques and technologies. This development was later transferred to the production of civilian goods and services. Today's warfare has not only a classical dimension but also a cybernetic one. And, it is the cybernetic advantage that often gives rise to the conventional advantage. One of the manifestations of cyber warfare is cyberattacks and cyber threats. The cybernetics industry, both those used to attack and those used to defend against attacks, is one of the fastest growing industries today. As a result, articles appear in the specialised press, encouraging investors to take an interest in cyber and IT companies.

Modern warfare is certainly changing the perception of high-tech, IT, and cyber companies. The use of drones itself shows that IT is crucial in such a war. Another expressions of this interest are the events related to cyberattacks, remote shutdown of equipment, data theft, destabilisation of banking systems, attacks on government institutions, etc. Any company dealing with high technologies is considered crucial in such conditions, and its solutions are analysed and implemented by decision-makers. The decision-makers themselves try to support and promote the development of cybernetic solutions and thus cyber companies.

It is against this background that the effectiveness of the activities of high-tech companies should now be assessed. Not every solution proposed by such companies is accepted by decision-makers or the market. This makes running such a business potentially very profitable, but also very risky. The research conducted in this thesis clearly shows that the mere fact that a company belongs to a group of companies involved in IT, cybersecurity, or high technology does not guarantee a successful investment. This can be seen in both American and Polish markets. However, taking into account the importance of the Russian-Ukrainian war in the company's strategy and implementing business solutions that take into account the economic changes caused by the war can contribute to greater market success. Investors should therefore critically assess the company's development potential and make decisions on this basis, rather than relying solely on press reports about the company's potential.

References

[1] R. Von Solms, J. Van Niekerk, "From information security to cybersecurity," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] W. Raghupathi, S.J. Wu, V. Raghupathi, "The role of information and communication technologies in global sustainability: A review," *Journal of Management for Global Sustainability*, vol. 2, no. 1, pp. 123–145, 2014.

[3] K.L.-T. Low, C.S. Lim, A. Samudhram, "Sustainable economic development: A perspective from ICT loops in developing nations," *African Journal of Business Management*, vol. 5, no. 15, pp. 6138–6149, 2011, doi: 10.5897/AJBM10.529.

[4] R.H. Courtney Jr., "A systematic approach to data security," *Computers & Security*, vol. 1, pp. 99–112, 1982, doi: 10.1016/0167-4048(82)90003-7.

[5] P. Dixon, D. Jorgenson, *Handbook of Computable General Equilibrium Modeling*, Elsevier, North Holland, 2012.

[6] M. McLennan, *The global risks report*, 16th ed. Geneva: World Economic Forum, 2021.

[7] J. Lewis, Z. Smith, E. Lostri. (2020). *The hidden costs of cybercrime*. [Online]. Available: https://www.csis.org/analysis/hidden-costs-cybercrime. [Accessed: Aug. 17, 2021].

[8] Verizon, *Data Breach Investigations Report,* 2020. [Online]. Available: https://itb.dk/wp-content/uploads/2020/07/verizon-data-breach-investigations-report-2020.pdf. [Accessed: Aug. 17, 2021].

[9] International Organization for Standardization, *Information technology – Security techniques – Code of practice for information security controls (AS ISO/IEC 27002:2015)*, 2015. [Online]. Available: https://www.iso.org/standard/43757.html. [Accessed: Aug. 17, 2021].

[10] P. Rathod, T.A. Hämäläinen, "A novel model for cybersecurity economics and analysis." 17th IEEE International Conference on Computer and Information Technology, 2017, pp. 274–279, doi: 10.1109/CIT.2017.65.

[11] E.M. Ahmed, "Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth," *Journal of the Knowledge Economy*, vol. 2, pp. 1–19, 2020, doi: 10.1007/s13132-020-00627-3.

[12] Statistics Poland. (May 10, 2024). *Macroeconomic Indicators*. [Online]. Available: https://stat.gov.pl/wskazniki-makroekonomiczne. [Accessed: May 17, 2024].

[13] H. Varian, "System reliability and free riding," in *Economics of information security*, L.J. Camp, S. Lewis, Eds., Dordrecht: Kluwer, 2004, pp. 1–15.

[14] R. Anderson, T. Moore, "Information security: Where computer science, economics and psychology meet," *Philosophical Transactions of the Royal Society a Mathematical, Physical and Engineering Sciences*, vol. 367, pp. 2717–2727, 2009, doi: 10.1098/rsta.2009.0027.

[15] Palo Alto Networks. (May 04, 2024). *Protect Against Russia-Ukraine Cyber Activity*. [Online]. Available: https://www.paloaltonetworks.com/russia-ukraine-cyber-resources. [Accessed: May 17, 2024].

Websites

https://www.lynxbroker.pl/inwestowanie/gielda/akcje/analiza-akcji/cyberbezpieczenstwo-5-propozycji-akcji. [Accessed: Jan. 12, 2024].

https://pfrsa.pl/aktualnosci/polski-sektor-cyberbezpieczenstwa-poznaj-startupy-ktore-poprawiaja-bezpieczenstwo-w-sieci.html. [Accessed: Jan. 10, 2024].

https://dnarynkow.pl/sektor-cyberbezpieczenstwa-najciekawszy-temat-inwestycyjny-dekady. [Accessed: Jan. 07, 2024].

https://gpwatak.pl/inne/cyberbezpieczenstwo-trend-w-najblizszej-przyszlosci. [Accessed: Jan. 12, 2024].

https://www.parkiet.com/analizy-rynkowe/art19680311-ukryte-perelki-w-sektorze-it. [Accessed: Jan. 07, 2024].

https://www.investors.com/news/technology/cybersecurity-stocks. [Accessed: Jan. 12, 2024].

https://www.fool.com/investing/stock-market/market-sectors/information-technology/cybersecurity-stocks. [Accessed: Jan. 11, 2024].

https://www.kiplinger.com/investing/stocks/tech-stocks/602685/cybersecurity-stocks-to-lock-up-growth. [Accessed: Jan. 10, 2024].

https://www.nasdaq.com/articles/6-cybersecurity-stocks:-which-is-the-best-to-buy. [Accessed: Jan. 07, 2024].

https://admiralmarkets.com/education/articles/shares/cybersecurity-stocks. [Accessed: Jan. 12, 2024].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Assessment of the Cybersecurity of Ukrainian Public Companies Listed on the Warsaw Stock Exchange S.A.

Anna Szczepańska-Przekota | Department of Finance, Faculty of Economic Sciences, Koszalin University of Technology, Poland | ORCID: 0000-0002-4002-5072

Abstract

Nowadays, the number of sophisticated cyberattacks targeting critical infrastructure or banking systems is increasing. Cases of successful attacks are not uncommon, as statistics in Ukraine demonstrate, and they are becoming more frequent and advanced. This results in an increased risk for companies listed on the stock exchange. The article provides examples of cyberattacks in Ukraine, including those using ransomware, attempts to infiltrate energy systems, and attacks on government institutions. It is noted that the presence of cyber threats is strongly linked to the political and international situation of the country. Analyses conducted focus on the examination of cyber threat events in Ukraine and their impact on the WIG_UKRAIN stock index from 2015 to 2023. The evaluation includes the index's return rates on the day of the cyber threat occurrence, the following day, and the average return rate within five sessions after the threat. An analogous study for the WIG index is adopted as a benchmark. Based on the obtained results, it can be said that before the year 2022, cyberattacks on Ukraine did not have a significant impact on the value of the Ukrainian company stock index. The situation changed after 2022, where each potentially economically harmful cyberattack contributed to the decrease in the value of Ukrainian-listed companies. Generally, the start of hostilities in 2022 significantly increased the volatility of the WIG_UKRAIN index quotations. This is to be expected, as markets react badly to uncertainty.

Received: 25.02.2024

Accepted: 22.05.2024

Published: 15.07.2024

Cite this article as:
A. Szczepańska-Przekota "Assessment of the cybersecurity of Ukrainian public companies listed on the Warsaw Stock Exchange S.A.," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190343

Corresponding author:
Anna Szczepańska-Przekota, Department of Finance, Faculty of Economic Sciences, Koszalin University of Technology, Poland.
E-mail: anna.szczepanska-przekota@tu.koszalin.pl;
0000-0002-4002-5072

Keywords

cybersecurity, cyberspace, cyber threat, WIG_UKRAIN index, WIG index

1. Introduction

The sectors of the economy, such as transportation, energy, healthcare, and finance, are becoming increasingly dependent on digital technologies in their core activities. The digital era creates vast opportunities and brings unparalleled economic growth, connecting businesses worldwide and supporting innovation. However, these interconnections have also exposed organisations and society to a constant threat of cyberattacks.

Cyberattacks are becoming more frequent and sophisticated throughout Europe. The surge in ransomware and cyberattacks increased by over 150% throughout the entirety of 2020. This signifies that cyber insurance is becoming a less profitable business for insurers [1]. According to forecasts, by 2025, as many as 41 billion devices worldwide will be connected to the Internet of Things. Therefore, decisive actions towards cybersecurity can enhance the credibility of digital tools and services, primarily ensuring the security of businesses operating in a cyber environment on a daily basis.

Ukrainian publicly traded companies, like many others worldwide, face the challenge of navigating the complex landscape of cybersecurity. The article presents the cybersecurity landscape of Ukrainian publicly traded companies, examining the threats they face, the measures they take, and the need for constant vigilance in the digital age.

The conducted analysis covers specific cases of cyberattacks, their complexity, economic consequences, and the financial market's response. The overview of events underscores the role of geopolitical situations in shaping the market's sensitivity to cyber threats. The ultimate aim is to provide a comprehensive understanding of how cyber threats impact the stock value of Ukrainian companies and to indicate potential remedial actions for businesses facing increasing cyber risks.

1.1. The Essence of Cybersecurity and Cyber Threats

In today's world, where technology plays a crucial role in all aspects of life, cybersecurity is becoming increasingly important for individuals, businesses, institutions, and nations seeking to effectively protect their digital assets from threats. It is worth noting that security is perceived as an objective state, characterised by the absence of threat, subjectively felt by individuals and groups [2]. In common understanding, security may denote a state in which an individual has a sense of certainty in a smoothly functioning legal and economic system. Security should not be treated as an independent variable, as it has a dynamic nature and can change due to complex phenomena [3].

Cybersecurity involves the resilience of information systems against actions that violate the confidentiality, integrity, availability, and authenticity of processed data or related services offered by these systems. The goal of cybersecurity is to secure information technology (IT) infrastructure, software, personal data, and ensure the integrity, availability, and confidentiality of information.

The communication space created by Internet-related linkages (cyberspace) is where processes threatening security are embedded. Cybersecurity threats are potential causes of incidents, and the vulnerability of an IT system is a characteristic that can be exploited by cybersecurity threats. According to the definition formulated by the US Department of Defense, cyberspace is a ‘global domain within the information environment consisting of the interdependent networks of information technology infrastructure (IT) and data contained therein, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers’ [4]. Thus, cyberspace constitutes a kind of communication space created by Internet-related linkages [5]. Analysing the features of this cyber space indicates that it is a unique technosystem of global social communication, shaped by the integration of forms of information transmission and presentation, leading to digitalisation and the creation of a global integrated teleinformatics platform [6].

The opposite of security is a state of threat, the nature of which is associated with an objective category of risk that always exists independent of human awareness. Awareness of threat becomes a key decision criterion in every area of human and economic entity functioning, subject to management [7]. In the literature of economics and finance, risk is defined differently [8, 9]. Events in the geopolitical sphere confirm that risk is embedded in a dynamic evolutionary model of the world. Risk is associated not only with the realisation of specific intentions but also with the desire to maintain the existing state of affairs, that is, not taking or refraining from certain actions [10].

It is different from uncertainty, which relates to events or changes that are difficult to estimate, and the probability is completely unknown [11]. This phenomenon has caused the number and severity of cyber threats in recent years to be unprecedented, and the costs of cyberattacks for corporate boards and other external and internal stakeholders are enormous. The consequences caused in cyberspace by unauthorised users lead to dangerous social and economic consequences. Institutions and companies are taking initiatives to protect data, critical business processes, and the availability and integrity of information systems. The constantly evolving cyber threats, including those related to the armed conflict in Ukraine and the recent acceleration of digitisation, are key factors driving the need to develop appropriate tools to increase organisations' capabilities in managing cybersecurity risk [12]. It is believed that cybersecurity needs to be incorporated at all levels of the company's business model, that is, both in operational and supporting processes.

In Poland, a significant legal act regulating aspects of cybersecurity is the Act on the National Cybersecurity System. According to the Security Strategy of the Republic of Poland for the years 2019–2024, a cybersecurity threat is any potential circumstance, event, or action that may cause harm, disruption, or otherwise adversely affect networks and teleinformatic systems, users of such systems, and other individuals, in accordance with the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on cybersecurity certification of Information and Communication Technology (ICT) products and repealing Regulation (EU) No. 526/2013 (the Cybersecurity Act).

According to the Threat Landscape Report – 2021 (ENISA Threat Landscape – 2021), the most significant cyber threats include the following:

- ransomware software,
- malicious software (malware),
- email-related attacks,
- threats related to data,
- threats related to availability and integrity,
- disinformation.

Vulnerability to cyberattacks is an objectively defined probability that the security system of an enterprise may be threatened. This indicates the likelihood of exploiting a gap in a specific security system. Refsdal et al. argue that cyber risk is not synonymous with every risk to which a cyber system may be exposed; cyber risk is limited to the risk caused by cyber threats [13].

The risk of server damage, such as flooding, is not a risk associated with cyberspace unless facilitated by a cyber threat. Examples of cyber threats include breaches of confidentiality through virus attacks in cyberspace and loss of availability due to denial-of-service (DoS) attacks.

The cybersecurity risk of an enterprise depends on various internal and external factors, including the size of the company's assets, the technology it employs, vulnerability to threats, awareness and competence of employees in security matters, cybersecurity procedures, supplier (outsourcing) security, the vulnerability of the overall infrastructure on which the enterprise operates, and the motivation of potential criminals. Considering all these factors and the limited knowledge about the impact of individual factors on the overall enterprise risk, understanding, and estimating cyber insurance risk is very complex. Simple metrics, such as the number of lost records, do not always correlate with the total cost of risks [14].

1.2. Cybersecurity Challenges in Ukraine

Ukraine, emerging as an economic powerhouse in Eastern Europe, boasts a growing number of companies listed on stock exchanges. However, the country's geopolitical situation has made it a primary target for cyberattacks. The ongoing conflict with Russia, which began in 2014, has complicated Ukraine's cybersecurity landscape. Cyberattacks, often attributed to state-sponsored entities, target critical infrastructure, government agencies, and private sector entities.

Ukrainian publicly traded companies may be particularly vulnerable to these threats. They must confront a series of cybersecurity challenges, such as the following:

- Phishing attacks, where cybercriminals use deceptive email messages and fake websites to persuade employees to disclose confidential information or install malicious software.
- Ransomware attacks crippling operations and demanding high ransoms.
- Vulnerabilities in supply chain security, as globalised companies rely on international supply chains, and cyberattacks on

partners or suppliers can have a cascading impact on Ukrainian enterprises.
- Politically motivated state-sponsored attacks that can result in significant financial damages.
- Internal threats where employees may intentionally or unintentionally breach cybersecurity measures.

Ukraine has experienced various forms of cybercrimes, both related to the conflict with Russia and stemming from the overall rise in global cyber threats. These include hacking attacks on critical infrastructure, attempting to infiltrate energy systems, telecommunications, or air traffic management systems. Such attacks can have serious consequences for public safety and the functioning of the state. Another form of cybercrime is data theft and attacks on government institutions, where hackers seek illegal access to sensitive data, such as citizens' personal information or classified government data. These attacks may be politically motivated, aiming to acquire confidential information or spread disinformation.

Financial systems are common targets for cybercriminals attempting to infiltrate banks and financial institutions to steal funds or manipulate financial systems. Ransomware attacks follow a similar pattern, infecting computer systems or networks and then demanding ransom in exchange for restoring access to data or systems. Companies, public institutions, and administrative entities may be targeted in such attacks. Attacks on the educational sector, such as schools, universities, and other educational institutions, are also prevalent due to the sensitive personal data of students and employees they store.

The Ukrainian government is taking actions to secure against these threats, but new cybercriminal techniques continue to emerge. Therefore, education, international collaboration, and continuous security system updates are crucial in combating these types of threats.

The extent and capabilities of non-state cyber actors became evident primarily during the Russian-Ukrainian war. According to Štrucl [15], the Russian Federation's previously successful hybrid warfare strategies faced challenges in the initial months of the 2022 war due to the active involvement of various hacking and hacktivist groups aligning themselves with the conflict. In the Ukrainian context, there seems to be an unspoken agreement among state institutions to allow non-state cyber actors to selectively carry out cyber defence functions. In February 2022, Ukrainian Deputy

Prime Minister M. Fedotov advocated for the establishment of the Information Technology Army of Ukraine. Hacktivist groups, such as Network Battalion 65, Elves, Cyber Guerrillas, Cloud Atlas, and notably, Anonymous, have been engaged in anti-Russian and anti-Belarusian activities, with Anonymous emerging as the most media-savvy cyber participant in the conflict [16].

1.3. Enhancing Cybersecurity Measures

In response to these threats, Ukrainian publicly traded companies increasingly recognise the importance of robust cybersecurity measures. Several strategies are employed to protect digital assets:

1. Organisations develop comprehensive cybersecurity policies and provide training to employees to raise awareness and promote best practices in cybersecurity.
2. Utilising high-quality software on end-user workstations, such as Endpoint Detection and Response (EDR) systems, helps secure and monitor computers, servers, and smartphones within the organisation. If any point in the IT system is infected, it is immediately isolated to prevent the attack from spreading to the entire corporate network and other devices.
3. Investments in advanced firewalls, intrusion detection systems, and endpoint protection are essential for safeguarding against cyber threats.
4. Developing and testing incident response plans is crucial for minimising the damage resulting from cyberattacks.
5. Companies conduct regular security audits and vulnerability assessments to identify and address weak points.
6. Collaborating with Ukrainian law enforcement and international partners can assist in effectively tracking and responding to cybersecurity threats.
7. Investing in employee education has a positive impact on the company's security levels. Hackers often initiate attacks by sending messages to ordinary employees, because there is a significant chance that such a person will click on an infected link. Awareness of cyber threats among employees varies and is usually lower than that of IT specialists. Regular training sessions enable the elevation of knowledge levels and the adoption of best practices, enhancing employees' resilience to hacker manipulations.

While these measures are essential, it is crucial to remember that the cybersecurity landscape is constantly evolving. Cybercriminals continuously develop new tactics and exploit vulnerabilities, requiring companies to maintain adaptability and vigilance. A proactive approach to cybersecurity is the most effective way to anticipate potential threats. Companies must also be aware of the regulatory environment. The Ukrainian government is working on cybersecurity regulations to strengthen legal frameworks for cybersecurity and data protection. Adhering to these regulations is not only a legal requirement but also a prudent cybersecurity practice.

Many studies show that cyberattacks, especially those directly targeting listed companies, cause significant damage [17]. This damage spreads throughout the industry [18]. As a result, investor confidence in such companies declines, the share price and hence the market value of the company falls, and share price volatility increases. There is usually a negative market reaction immediately after the attack [19]; the markets do not wait for the effects of such attacks to be determined. These are all negative phenomena. There is no positive market reaction to cyberattacks. In the long run, the situation can go one of the two ways: if the company tries to counter the attack, it can stay in the market [20]; technology companies are usually better prepared for attacks than companies in other industries [21]; if it does not take action, then it risks being taken out of the market [22].

2. Methods

The subject of the study is cyber threat events in Ukraine and their impact on the quotes and returns of the WIG_UKRAIN index during the period from December 2015 to December 2023 on the Warsaw Stock Exchange (GPW) S.A. Analyses conducted focus on the examination of cyber threat events in Ukraine and their impact on the WIG_UKRAIN stock index from 2015 to 2023. The evaluation includes the index's return rates on the day of the cyber threat occurrence and the average return rate within sessions after the threat. According to the efficient market hypothesis, any event that could affect the valuation of financial instruments is discounted in the market price. Cyber threats are considered information that could potentially influence the value of financial instruments. Of course, cyber threats vary in type and scope of impact. Therefore, a review of selected cyber threats was conducted, and an assessment of their impact on the value of the Ukrainian companies' index was made. The returns of the index were observed on the following events:

1. The day of the cyber threat occurrence.
2. The day immediately following the cyber threat occurrence.
3. The average return over five sessions following the cyber threat occurrence.

The performance of the WIG stock index was chosen as a reference point, for which corresponding returns were determined. During the period under review, the average volatility of the WIG_UKRAIN index quotations was compared with the WIG index quotations. Low rates of return were considered as the negative effect of reducing the value of Ukrainian-listed companies as a result of cyber activities. The WIG-Ukraine index is the second national index calculated by the stock exchange. It includes companies listed on the Warsaw Stock Exchange (GPW) whose headquarters or central offices are located in Ukraine or whose activities are predominantly conducted in this country. The first value of the index was published on 4 May 2011. Historical values of the index were recalculated from the base date of the index, which is 31 December 2010, when the index value was 1000 points. WIG-Ukraine is an income index, considering both prices of the stocks included and income from dividends and rights issues in its calculation.

On the other hand, the Warsaw Stock Exchange Index (WIG) encompasses stocks of companies listed on the primary market. It is the longest-standing index on the Warsaw Stock Exchange (GPW), calculated since 16 April 1991. WIG is an income-type index, meaning that its calculation takes into account both prices of the stocks included and income from dividends and rights issues. It also expresses the relative total value of the companies present on the Warsaw Stock Exchange (GPW) in relation to their value at the beginning of the index listing.

The main limitation of the research is the difficulty in determining the date of publication of information about a cyberattack. Several key dates there: the date of preparation of the cyberattack, the date of the cyberattack, the date of information about the cyberattack, and the date of reaching the market. Each of these dates is critical, but none can be determined with complete accuracy. It is often necessary to act on the basis of residual information. In addition, the number and nature of all cyberattacks are not known, so it is necessary to focus on a few.

3. Results

The onslaught of attacks on information systems using malicious software, such as ransomware, is immense, and furthermore, the size of the hacker arsenal is increasing. History shows that the actions of cybercriminals vary depending on the political, economic, and international situation in Ukraine. In most cases, these actions aimed to acquire confidential information related to Ukraine's politics, defence, or economy.

3.1. Examples of Cyberattacks on Ukraine

Examples of cyberattacks have been compiled in Table 1.

Table 1. Examples of cyberattacks on Ukraine.

Date	Type of threat	Consequences
23 December 2015	• Attacks on the energy sector – APT Sandworm.	• Power outages affecting approximately 230,000 consumers for 1–6 h. • Preventing customers from calling to report emergencies – malfunction of 16 telephone line substations. • Attempt to undermine trust in Ukrainian energy companies and the government.
17 December 2016	• Before the cyber incident, cybercriminals conducted a 'denial of service' phone attack on customer service centres.	• Over an hour-long blackout. • Power outage led to the loss of about one-fifth of energy consumption in Kyiv at that time of night. • Disruption of power distribution, cascading failures, and equipment damage.
23 & 28 December 2016	• Malicious software. The Security Service of Ukraine (SBU) apprehended Russian special service officers who attempted to damage a series of computer networks in infrastructure facilities in Ukraine.	• SBU discovered malicious software on the computers of regional operators of power grid networks. The virus attack was coordinated with a flood of phone calls to the hotline of several energy companies.
27 July 2017	• Attack on public, financial, and energy sectors. • Attack using malicious software for data erasure, known as NotPetya. The attack is described as the 'most destructive cyberattack in history'.	• The radiation monitoring system at the Ukrainian nuclear power plant in Chernobyl was shut down. • Economic loss for Ukrainian entities due to irreversible data encryption. • Infiltration of computer networks, including systems of the National Bank of Ukraine, Kyiv-Boryspil International Airport, and the capital's metro. • Affected 65 countries and approximately 49,000 systems worldwide. • Estimated global economic losses exceeding US$10 billion.
11 July 2018	• 'VPN Filter' attack on the chlorine distillation system.	• Cyberattack on the network devices of the Chlorine Distillation Station in Auly, which supplies liquid chlorine to water and sewage treatment plants in 23 provinces of Ukraine as well as Moldova and Belarus.
13 January 2022	• Virus attacks (ransomware) erasing data, known as 'WhisperGate', targeting all sectors of the economy.	• Microsoft has identified a destructive operation of malicious software (labelled as WhisperGate) targeting multiple organisations in Ukraine. It is designed to appear as ransomware, but lacks a ransom recovery mechanism and is intended for the destructive shutdown of targeted devices, rather than extortion. The victims include various government, non-profit, and IT organisations.

(*continues*)

Table 1. Continued.

Date	Type of threat	Consequences
14 &15 January 2022	• Hacker attack on government websites, Ministry of Education, State Emergency Service, government, Ministry of Energy, and the government application Dija, which allows for the use of documents in digital form and access to some public services. • Alteration of content on government websites – Belarus APT Group – UNC1151.	• Because of the attack, government websites temporarily ceased to function. The goal was data cleansing. • The attack paralysed a significant portion of the government's digital public infrastructure, including the most frequently used website for handling online government services, Diia. Diia also plays a role in responding to the coronavirus in Ukraine and encouraging vaccinations. The application also disabled the headquarters of the cabinet of ministers, ministries of energy, sports, agriculture, veterans affairs, and ecology.
15 & 16 February 2022	• Distributed denial-of-service (DDoS) attack on websites of financial and public sectors. • DDoS attack described as the largest to date in Ukraine.	• At least 10 Ukrainian websites were inaccessible, including the Ministry of Defence, Ministry of Foreign Affairs, and two largest state-owned banks. • Bank customers reported issues with online payments, banking apps, and, in very few cases, accessing ATMs. • These attacks were associated with fake SMS messages sent to Ukrainian phones to induce panic.
22 February–7 March 2022	• Phishing and DDoS attacks targeting Ukrainian entities in the public, military, and information sectors – FancyBear/APT28, Ghostwriter/UNC1151, Mustang Panda, or Temp.Hex.	• Exposure of information enabling the identification of individuals. • Restriction of access to information. • Destabilisation of civil infrastructure.
24 February 2022	• DDoS attack on the news website. • Malware attack. • 'IsaacWiper' on government entities. • Phishing campaign targeting the public sector delivering the 'SunSeed' malware.	• A DDoS attack paralysed The Kyiv Post's systems, forcing them to find alternative ways of publishing news by posting shortened articles on Facebook, Twitter, and LinkedIn. There were logistical issues related to the non-functioning personnel system and significantly more challenging communication between employees. • ESET, s.r.o., identified another cleansing element in Ukrainian government's networks that affects organisations not targeted by HermeticWiper and has no similarity in code. On 25 February 2022, the attackers released a new version of IsaacWiper with debugging logs, indicating that the attackers were unable to wipe some of the compromised computers.
2 February 2022	• Cyberattack on a border control checkpoint. • Websites of Ukrainian universities targeted – Brazil Threat Actor Group – theMx0nday. • Attack on a satellite Internet service.	• At a Ukrainian border control post, a cyberattack occurred involving data deletion, slowing down the process of allowing refugees to enter Romania. • 25 February 2022 – Attacked websites of Ukrainian. universities – Brazil Threat Actor Group – theMx0nday. • Cyber incident – an attack on the satellite Internet service Viasat caused a partial network outage for customers in Ukraine and beyond in Europe who rely on its KA-SAT satellite.

(*continues*)

Table 1. Continued.

Date	Type of threat	Consequences
28 February 2022	• Attacks by the Trojan 'Foxblade' (aka HermeticWiper) on public/private sector and military. Microsoft has detected a new series of offensive and destructive cyberattacks targeting Ukraine's digital infrastructure. These include attacks on the financial sector, agriculture, crisis response services, humanitarian aid as well as organisations and enterprises in the energy sector.	• Difficulties in civilian access to finances, food, and energy sources. • Destabilisation of civil infrastructure. • Disinformation. • Attempted theft of information enabling the identification of individuals associated with health, insurance, and transportation as well as other sets of government data.
4 March 2022	• Malware attacks on non-governmental organisations.	• Malicious software was specifically targeted at charitable organisations, non-governmental organisations, and other aid organisations to spread confusion and cause disruptions. • The aim of the attack was to disrupt the delivery of medicines, food, and clothing during the armed conflict.
29 March 2022	• Cyberattack on the IT infrastructure of Ukrtelecom.	• Hacker attack on Ukrainian websites. Because of the breach, some internal systems were reset, leading to the loss of access for certain local subscribers.
12 July 2023	• Malware attacks on diplomats in Kyiv.	• The hackers targeted at least 22 out of approximately 80 foreign missions in Kiev. Hackers from the group known as APT29 or 'Cozy Bear' intercepted and copied a car sale offer from one of the Polish diplomats. Subsequently, they embedded malicious software in it and sent it to dozens of other diplomats stationed in Kiev.

Sources:
https://stinet.pl/ukraina-historia-cyberatakow-cz-1-2/. [Accessed: Dec. 30, 2023];
https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8333044,ukraina-hakerzy-atak-strony-rzadowe.html. [Accessed: Dec. 30, 2023];
https://www.money.pl/gospodarka/cyberatak-hakerow-na-ambasady-w-kijowie-wykorzystali-oferte-sprzedazy-samochodu-6918742318898016a.html. [Accessed: Dec. 30, 2023];
https://www.pap.pl/aktualnosci/news%2C1089376%2Czmasowany-atak-hakerski-na-ukrainie-nie-dzialaja-strony-wielu-organow. [Accessed: Dec. 30, 2023].

Among the cyberattacks on Ukraine, actions with a sabotage character have been documented. These attacks were carried out to disrupt the normal functioning of critical infrastructure systems, such as power plants, energy systems, or telecommunications. Cyberattacks have intensified significantly since Russia declared war on Ukraine. The DDoS attack from February 2022 is considered the largest to date in Ukraine. Many Ukrainian websites, such as those of banks, government, and the military, were inaccessible.

Temporarily, the websites recovered within a few hours. Such actions indicate an intention to instigate panic. This type of attack is aimed at disorganising the military, disrupting communication, and manipulating information.

3.2. The impact of cyberattacks on the volatility of the WIG_UKRAIN index

Some attacks aimed at disrupting the normal functioning of the government, creating chaos in society, or undermining trust in public institutions. The consequences of such actions involve not only manipulating information but also influencing public opinion at home and abroad.

It is worth emphasising that the motives behind attacks on Ukraine were complex and involved a combination of different objectives. Moreover, the scale and type of attacks change depending on the developments on international stage.

Figure 1 depicts the performance of the WIG_UKRAIN and WIG indices. Selected cyberattacks are marked with red arrows. The trends in which both indices were examined are generally in agreement. The correlation coefficient for the levels of quotations in the examined period is 0.3369. Its not very high value is primarily influenced by the period after Russia's aggression on Ukraine when initially both indices lost value. However, since the end of 2022, the WIG index entered a strong upward phase, while the WIG_UKRAIN index continues to lose value. It is challenging to expect an increase in the value of the index of Ukrainian companies operating in such difficult times under uncertain political and economic conditions.

Table 2 presents return rate statistics during the period of a cyberattack and the period following the cyberattack. Throughout the entire period, the WIG_UKRAIN index experienced an average decrease of 0.0020% per session, while the WIG index saw an average increase of 0.0309% per session. The provided statistics allow for the distinction of two sub-periods, that is, until 2022 and from 2022 onwards. Before 2022, the changes were not as significant as they were after 2022. Generally, the commencement of military actions in 2022 significantly increased the volatility of WIG_UKRAIN index quotations, which is an expected situation, as markets tend to react poorly to uncertainty.

Cyberattacks in Ukraine until 2022 did not inflict significant damage on the value of the index of Ukrainian companies. The attack

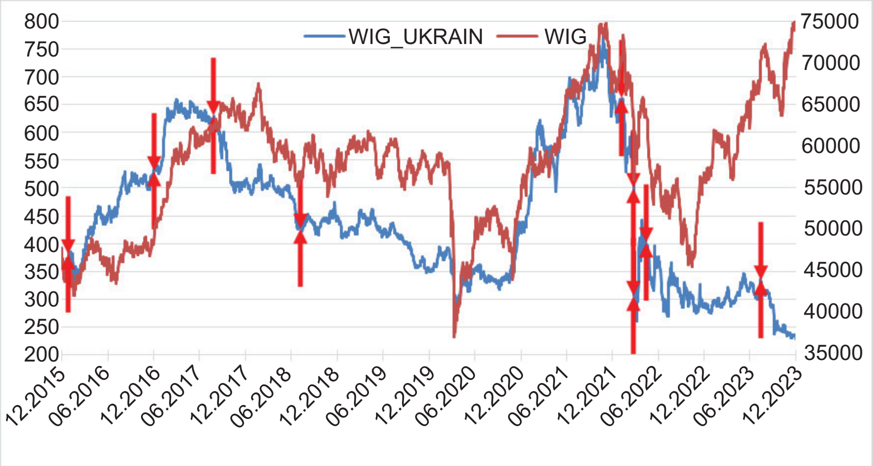


Figure 1. Performance of the WIG_UKRAIN and WIG indices from December 2015 to December 2023. *Explanations*: left axis – WIG_UKRAIN; right axis – WIG.
Source: Own compilation based on Warsaw Stock Exchange (GPW) data.

Table 2. Return rate statistics.

Cyberattacks	WIG_ UKRAIN			WIG		
	Mean –0.0020%			Mean 0.0309%		
	Day	Next day	5-Day mean	Day	Next day	5-Day mean
23 December 2015	0.66%	0.68%	0.96%	0.31%	0.00%	–0.46%
17 December 2016	–1.37%	0.19%	–0.53%	0.03%	0.70%	0.07%
23 December 2016	–0.25%	0.69%	0.38%	–0.25%	0.14%	0.13%
28 December 2016	1.06%	–0.07%	0.66%	–0.08%	0.73%	0.45%
27 July 2017	0.72%	0.85%	–0.08%	–0.31%	0.31%	0.02%
11 July 2018	0.07%	–0.17%	–0.03%	–0.87%	0.23%	–0.20%
13 January 2022	0.41%	–2.41%	–1.93%	–0.12%	–0.93%	–0.72%
14 & 15 January 2022	–2.41%	–1.93%	–1.99%	–0.93%	–0.43%	–0.92%
15–28 February 2022		–2.39%			–0.67%	
4 March 2022	–6.97%	–12.28%	–1.20%	–4.30%	0.30%	–0.37%
29 March 2022	15.80%	–5.31%	2.35%	1.58%	0.47%	0.35%
12 July 2023	–0.04%	0.86%	0.52%	2.55%	0.10%	1.00%

on the energy sector conducted on 17 December 2016 caused maximum damage to the index. In this case, the statistics of the WIG_UKRAIN index compared to WIG look significantly worse. Any other highlighted cyberattack in the period until 2022 did not result in a permanent loss of value for the WIG_UKRAIN index, compared to WIG. One could even say that the market did not react to such cyberattacks. Moreover, even the attack on 27 July 2017, which was considered the largest in history at that time, remained practically unnoticed by the stock exchange.

The situation changed from 2022 onwards. With the onset of military actions, the stock market became significantly more sensitive to any information coming from Ukraine. The average change in the value of the WIG_UKRAIN index from February 2022 to the end of 2023 was -0.1195% per session. Meanwhile, during periods of intensified cyberattacks, especially the day after an attack, return rates reached significantly lower values. Only the attack on 12 July 2023 had a minor impact, but it was an attack without significant economic importance. However, every attack with potentially severe economic consequences from 2022 contributed to decline in the value of Ukrainian-listed companies

4. Conclusions

The global geopolitical situation plays a significant role in shaping global financial markets. Financial market sensitivity refers to the ability to respond to various factors, such as changes in the economy, political events, volatility in commodity prices, or factors disrupting the sense of security in a country. Rise in international tensions, conflicts, international negotiations, and political changes particularly impact the sensitivity of the stock market. The geopolitical situation in Ukraine has exposed entities operating in the capital market to increased cyberattack risks. However, companies are increasingly aware of the importance of investing in cybersecurity measures to protect their operations, data, and reputation. Ukrainian-listed companies must maintain a proactive approach to cybersecurity, continually adapting to new threats and changing regulations. Collaboration with governmental and international entities, comprehensive employee training, and the implementation of advanced cybersecurity technologies are crucial in the current efforts to protect Ukraine’s economic well-being in the digital age.

A review of selected cyberattacks on Ukraine, characterised as sabotage, indicates that the primary targets were critical infrastructure, such as power plants, energy systems, and telecommunications. The intensity of these attacks has increased since Russia declared war on Ukraine. The attacks had complex motives, such as disrupting government operations, creating social chaos, and undermining trust in public institutions. The goals also involved disrupting the armed forces, interfering with communication, and manipulating information.

Disruptive cyberattacks have resulted in the hindrance of telecommunications and the Internet services, restricted access to financial resources, and disrupted flow of news, and historically, they have been demonstrated to cause the denial of access to essential utilities, such as electricity, heating, and water. For instance, an incident on 29 March 2022 targeted Ukrtelecom, resulting in a connectivity collapse to only 13% of pre-war levels, causing nationwide disruption. The dissemination of false information and propaganda, often executed through attacks on the media sector, has a destabilising impact by influencing the information landscape and limiting the public's access to timely, trustworthy, and official information. This erosion of reliable information undermines trust in institutions through the manipulation of information. Furthermore, the compromise of data, including hacking and leaks facilitated by hacktivist groups, has led to the widespread publication of substantial volumes of organisational and individual data online, with potential unknown long-term consequences.

Cyberattacks not only led to information manipulation but also influenced public opinion both domestically and internationally. They stirred uncertainty, weakened trust in institutions, and affected societal stability.

An analysis of stock indices (WIG_UKRAIN and WIG) suggests that the market became more sensitive to information related to attacks from 2022 onwards, especially after Russia's aggression against Ukraine. Before 2022, cyberattacks on Ukraine had no significant impact on the value of Ukrainian company indices, except for the attack on the energy sector in December 2016. The situation changed from 2022 onwards, where every potentially economically harmful attack contributed to the decline in the value of Ukrainian-listed companies. With the onset of military actions, the stock market reacted more dynamically to cyberattacks. The returns of Ukrainian-listed companies reached lower values in the days following attacks, indicating increased market sensitivity to events related to the conflict.

Based on the conducted analyses, it is concluded that cyberattacks on Ukraine had a significant impact not only on infrastructure but also on financial markets and public opinion, especially after the start of military actions. The observed dependency confirms the growing sensitivity of the stock market to events related to cybersecurity. The Ukrainian government is taking steps to secure against cyber threats; however, education, international collaboration, and regular system updates remain crucial in combating such attacks.

It is important to underscore the importance of the effectiveness of cyber defence by Ukraine in repelling attacks and/or mitigating their impact [23]. Ukraine bolstered the resilience of its national ICT infrastructure and cyber incident response prior to and during the war, in cooperation with allied governments and private companies [24]. Ukraine's private sector has also largely contributed to this process [25]. This included activities to strengthen the cyber resilience of Ukraine prior to and since the 2014 and 2022 military invasions, and cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [26]. Ukraine's preparation, recognising that it has been the subject of cyberattacks for many years, has involved private–public partnerships. With the outbreak of the war, private actors, such as Microsoft, Google, Amazon, and ESET, s.r.o., have publicly acknowledged the role played in terms of tracking and forecasting cyber threats [27], hosting of governmental data in the public cloud outside Ukraine, and other forms of collaboration by the Government of Ukraine to thwart cyber threats [28–31].

References

[1] T. Johansmeyer. (2022). *The cyber insurance market needs more money.* Harvard Business Review. [Online]. Available: https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money. [Accessed: Dec. 27, 2023].

[2] H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*. Cracow: EAS, 2004.

[3] K. Chałubińska-Jentkiewicz, "Cyberbezpieczeństwo – Zagadnienia definicyjne," *Cybersecurity and Law*, vol. 2, no. 2, pp. 7–23, 2019, doi: 10.35467/cal/133828.

[4] J. Wasielewski, "Zarys definicyjny cyberprzestrzeni," *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 5, no. 5, pp. 225–234, 2013.

[5] J. Kisielnicki, *Systemy informatyczne zarządzania*. Warsaw: Placet, 2009.

[6] P. Sienkiewicz, "Terroryzm w cybernetycznej przestrzeni," in *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioło, J. Kisielnicki, K. Rajchel, Eds., Warsaw: Wyższa Szkoła Informatyki, Zarządzania i Administracji, 2009.

[7] A. Karmańska, M. Łada, "Ujawnianie obszarów i czynników ryzyka w sprawozdaniach z działalności spółek giełdowych – Obserwacje wobec zmian regulacji prawnych," *Zeszyty Teoretyczne Rachunkowości*, vol. 103, no. 159, pp. 42–43, 2019, doi: 10.5604/01.3001.0013.3074.

[8] M. Bochenek, “Ryzyko i niepewność w naukach ekonomicznych – Rozważania semantyczne,” *Ekonomia (Economics)*, vol. 21, no. 4, pp. 46–63, 2012.

[9] N. Iwaszczuk, *Ryzyko w działalności gospodarczej: Definicje, klasyfikacje, zarządzanie*. Cracow: IGSMiE PAN, 2021.

[10] K. Marcinek, *Ryzyko projektów inwestycyjnych.* Katowice: University of Economics in Katowice, 2001.

[11] C.L. Pritchanel, *Zarządzanie ryzykiem w projektach*. Warsaw: WIG-Press, 2002.

[12] E. Haapamäki, J. Sihvonen, “Cybersecurity in accounting research,” *Managerial Auditing Journal*, vol. 34, no. 7, pp. 808‒834, 2019, doi: 10.1108/MAJ-09-2018-2004.

[13] A. Refsdal, B. Solhaug, K. Stølen, *Cyber-risk management*. Series: Springer Briefs in Computer Science, Springer Cham, 2015.

[14] NetDilgence. (2014). *Netdiligence cyber claims study 2014*, Technical report, NetDilligence. [Online]. Available: https://netdiligence.com/. [Accessed: Dec. 29, 2023].

[15] D. Štrucl, “Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare,” *Contemporary Military Challenges*, vol. 24, no. 2, pp. 103–123, 2022. doi: 10.33179/BSV.99.SVI.11.CMC.24.2.6.

[16] D. Svyrydenko, W. Możgin, “Hacktivism of the anonymous group as a fighting tool in the context of Russia’s war against Ukraine,” *Future Human Image*, vol. 17, pp. 39–46, 2022. doi: 10.29202/fhi/17/6.

[17] M.C. Arcuri, M. Brogi, G. Gandolfi, “The effect of cyberattacks on stock returns,” *Corporate Ownership & Control*, vol. 15, no. 2, pp. 70–83, 2018, doi: 10.22495/cocv15i2art6.

[18] R. Jamilov, H. Rey, A. Tahoun. (Jun. 03, 2021). *The anatomy of cyber risk.* Working paper 28906, National Bureau of Economic Research, Cambridge. [Online]. Available: http://www.nber.org/papers/w28906. [Accessed: Dec. 27, 2023].

[19] M. Xu, Y. Zhang, “Data breach CAT bonds: Modeling and pricing,” *North American Actuarial Journal*, vol. 25, no. 4, pp. 543–561, 2021. doi: 10.1080/10920277.2021.1886948.

[20] M.C. Arcuri, L. Gai, F. Ielasi, E. Ventisette, “Cyber attacks on hospitality sector: Stock market reaction,” *Journal of Hospitality and Tourism Technology*, vol. 11, no. 2, pp. 277–290, 2020, doi: 10.1108/JHTT-05-2019-0080.

[21] S. Tweneboah-Kodua, F. Atsu, W. Buchanan, “Impact of cyberattacks on stock performance: A comparative study,” *Information and Computer Security*, vol. 26, no. 5, pp. 637–652, 2018, doi: 10.1108/ICS-05-2018-0060.

[22] K.T. Smith, L.M. Smith, M. Burger, E.S. Boyle, “Cyber terrorism cases and stock market valuation effects,” *Information and Computer Security*, vol. 31, no. 4, pp. 385–403, 2023, doi: 10.1108/ICS-09-2022-0147.

[23] Microsoft. (Jun. 22, 2022). *Defending Ukraine*: *Early lessons from the cyber war*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. [Accessed: Feb. 20, 2024].

[24] S. Landau. (Sep. 30, 2022). *Cyberwar in Ukraine*: *What you see is not what’s really there.* Lawfare. [Online]. Available: https://www.lawfareblog.com/

cyberwar-ukraine-what-you-see-not-whats-really-there. [Accessed: Feb. 20, 2024].

[25] E. Schroeder, S. Dack. (Feb. 27, 2023). *A parallel terrain*: *Public-private defense of the Ukrainian information environment*. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-privatedefense-of-the-ukrainian-information-environment/. [Accessed: Feb. 20, 2024].

[26] State Service of Special Communications and Information Protection of Ukraine. (Jan. 19, 2023). *Ukraine has signed an agreement on accession to the NATO.* Cooperative Cyber Defence Centre of Excellence. [Online]. Available: https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-zkiberoboroni-nato. [Accessed: Feb. 20, 2024].

[27] Microsoft. (Jun. 22, 2022). *Defending Ukraine*: *Early lessons from the cyber war*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. [Accessed: Feb. 20, 2024].

[28] G. Corfield. (Jan. 7, 2023). *Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft.* [Online]. Available at: https://www.telegraph.co.uk/business/2023/01/07/russian-cyberattacks-ukraine-halved-help-amazon-microsoft/. [Accessed: Feb. 20, 2024].

[29] S. Pell. (Dec. 1, 2022). *Private-sector cyber defense in armed conflict.* [Online]. Available: https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict. [Accessed: Feb. 20, 2024].

[30] I. Sánchez Cózar, J.I. Torreblanca. (Mar 7, 2023). *Ukraine one year on*: *When tech companies go to war*, European Council on Foreign Relations. [Online]. Available: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/. [Accessed: Feb. 20, 2024].

[31] J. McLaughlin. (Mar. 3, 2023). *Russia bombards Ukraine with cyberattacks, but the impact appears limited*. [Online]. Available: https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited. [Accessed: Feb. 20, 2024].

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Stronger Together? EU Support for Ukrainian Local Authorities Facing Cyber Attacks (2022–2023)

Iryna Fyshchuk | Department of Political Science and Management, University of Agder, Norway | ORCID: 0000-0002-7645-3490

Abstract

This study attempts to explore the extent to which EU support during the decentralisation process in Ukraine facilitates local authorities' digitalisation and strengthens their resilience against cyber attacks. The Ukrainian cyber attack cases are becoming more frequent in 2022 and 2023 in terms of war, especially on the websites of local authorities. The article demonstrates that decentralisation with the support of the EU-funded U-LEAD assistance programme provides an opportunity to bring state services closer to citizens and, accordingly, increase the efficiency of their provision. Decentralisation and digitalisation go hand in hand in the process of implementation in Ukraine. The digitalisation in this direction of local administrations becomes a tool for achieving this goal because it allows local administrations to offer more of their services in a digital format, which ensures the resilience of the development of local authorities. At the same time, the local authorities are less protected against cyber attacks, especially during the war. The article employs a semi-structured interview method to analyse data, revealing that representatives from local authorities participate in various training courses to enhance cybersecurity skills. However, the challenges vary and include issues such as lack of personnel, lack of funding, complex application procedures, lack of coordination, and technical capacity limitations. Indeed, Ukraine is still in the process of improving its own model of cyber defence

Received: 12.02.2024

Accepted: 24.05.2024

Published: 23.07.2024

Cite this article as:
I. Fyshchuk "Stronger together? EU support for Ukrainian local authorities facing cyber attacks (2022–2023)," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190344

Corresponding author:
Iryna Fyshchuk, Department of Political Science and Management, University of Agder, Norway. E-Mail: irafyshchuk@gmail.com; 0000-0002-7645-3490

for local authorities and the country as a whole in terms of countering Russian aggression, using among others practices of NATO and EU countries in the specified field.

Keywords

cyber attacks, cybersecurity, local authorities, digitalisation, decentralisation, EU

1. Introduction

Against the background of the ongoing full-scale Russian invasion of Ukraine and geopolitical tensions, at the same time, Ukrainian local authorities are in the treacherous territory of cyber attacks, as well as fulfilling integration requirements to the European Union. Cyber attacks are increasing, and local governments are often under-resourced and underprepared for them as indicated by Frandell et al. [1]. Moreover, cyber attacks actions aim to obtain sensitive information, disclose it, and threaten to publish or self-publish classified information about the state's information infrastructure [2]. The difficulties that large governments are having in this regard suggest that municipalities, especially small- to medium-sized ones, may also be struggling to protect their and their citizens' data [3]. At the same time, social media platforms, owned and operated by third parties, introduce potential threats such as accidental private data disclosure, misinformation spread, and hacks mentioned by Kenney [4]. As an example, during 13–14 January there was a global cyber attack on Ukrainian government websites. The websites of the Ministry of Education and Science, the Ministry of Foreign Affairs, the State Emergency Service, the Cabinet of Ministers, the Ministry of Energy, and 'Diia' (a mobile application developed by the Ministry of Digital Transformation of Ukraine for Ukrainian citizens) were not working. The attack presented a step towards the imminent Russian invasion on February 24.

Destructive attacks are a component of Russian wartime cyber operations [5]. Cyber attacks continue and threaten the well-being of the civilian population, and their amount is increasing at the local governments and more heavily impacted by cyber incidents than before. The combination of cyber- and physical attacks was aimed at disrupting the functioning of the Ukrainian government, municipalities and the army, undermining the public's faith in these institutions, damaging objects of critical infrastructure, and causing irreversible catastrophic consequences [6]. And under the conditions of the current decentralisation, local authorities have received more powers, but at the same time this a transitional stage and creates certain challenges. Decentralisation processes are related to digitalisation processes, which started at the same time and take place in parallel. Whereas digitalisation processes are aimed at improving administrative services at the state and the local level where the implementation is main.

The ongoing decentralisation process in Ukraine is considered one of the most successful reforms in the country so far highlighted by Pintsch [7]. Decentralisation of public authorities is a mechanism that ensures the sustainable development of regions of the state on the basis of the legislative and regulatory transfer of functions, powers and budgets from the central executive bodies to the local self-government bodies [8]. The development of the state and decentralisation situation is a transfer of powers and resources to lower levels of public administration. In addition, decentralisation stands out as one of the forms of development of democracy, which allows the state and its institutions to expand local self-government. Also, decentralisation allows to activation of the population for decision-making and implementing solutions for their own needs and interests. Furthermore, decentralisation narrows the sphere of influence of the state on society, replacing this influence with self-regulation mechanisms developed by society itself, which reduces the expenses of the state and taxpayers for the maintenance of the state apparatus indicated by Lukin et al. [9].

A review of the literature proves significant scientific interest researchers to study various aspects of decentralisation of the modern state, challenges and problems of decentralisation processes, and administrative and territorial reform. Rhodes and Bevir determine the general methodological principles of the theory of decentralisation, they proposed by Wagenaar (2014) the ‘distinctive interpretive theory’ [10]. Some of the scientists such as Dyer and Rose [11] that mentioned the successful implementation of decentralisation depends on strengthening the potential of local bodies’ power and the government’s capacity for assistance and supporting decentralisation. It is important that local authorities and, communities make the most of their territorial features, even if they are unfavourable that was highlighted by Mikuš et al. [12].

2. Methods

This article is based on the method of qualitative semi-structured interviews with a diverse group of 19 content experts, which were conducted between May 2023 and May 2024. The participants are established IT and cyber specialists, decision-makers in local authorities and central government bodies, politician leaders, professors, and researchers at universities, community managers, representatives of the cybersecurity charity funds, and NGO managers as shown in Table 1. Also, it was analysed official reports from the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU) [13], Microsoft Digital Defense Reports [14], Cybersecurity Tech Accord [15], and published interviews of leaders of the SSSCIPU, and media reports about cyber attacks in Ukrainian, including the observation of the social network platform as the official telegram channel of the State Special Communications.

The interviews reported in this article were initiated and organised within the framework of the project 'Digital transformation in Ukraine and EU integration', which investigates the EU support for

Table 1. Semi-structured interviews with a diverse group of experts

Interview	Description
I – 1	Decision makers
I – 2	Digital leader of the community
I – 3	IT Manager
I – 4	Cybersecurity specialist
I – 5	Politician
I – 6	Cyber specialist
I – 7	Professor
I – 8	Researcher
I – 9	Manager at the local authority
I – 10	Decision maker
I – 11	Public organisation manager
I – 12	Manager of the NGO
I – 13	IT specialist
I – 14	IT specialist
I – 15	Decision maker
I – 16	Community manager
I – 17	IT specialist
I – 18	Decision maker
I – 19	IT specialist

Ukrainian local authorities facing cyber attacks during 2022–2023. The geographical representation of the respondents is as follows – from the central part of Ukraine and north – 8 local authorities, south – 5, west – 4, and east – 2.

Due to the sensitivity of the topic, it was difficult to arrange interviews. The most commonly given reasons for non-response were restrictions on official duties as public servants and martial law, fear of participating in the interview, lack of time, and refusal without giving a reason. Indeed, almost 85% of the respondents expressed appreciation for its timeliness and relevance. The selection is based on the respondent`s willingness to participate in the interview. Most of the interviews took about one hour. The collection, storage, and analysis of the interview data are based on compliance with ethical standards and protection of the rights of the interview participants regarding voluntary participation, anonymity, and confidentiality.

3. Decentralisation and digitalisation processes in Ukraine

It is worth noting that the process of decentralisation and digitalisation did not begin almost in parallel since 2019. Indeed, in Ukraine, from the very beginning of its declaration of independence in 1991, the issue of decentralisation of power occupied a rather important place, since there was a strong centralisation of power in relation to decision-making. After the Orange Revolution, in 2004, changes were made to the Constitution of Ukraine and the governmental system changed from presidential-parliamentary to parliamentary-presidential. In 2010, the system was changed back to president-parliamentary, and after the Revolution of Dignity in 2014, the issue of changes was raised again, and the form of government got back to parliamentary-presidential. In addition, a thorough decentralisation process started in 2014.

As a matter of fact, Ukraine has established European integration as its main political course and a decentralisation process for making changes inside the country. Practically it chose a ‘partnership’ model of local self-government, under which the state recognises the increased importance of the territorial community as a carrier of direct democracy and a full-fledged living environment for citizens. According to the European Charter of Local Self-Government, which was adopted in 1985 and entered into force in 1988, the parties must guarantee the political, administrative, and financial independence of local authorities [16]. Additionally, Article 2 of this charter, it is mentioned that ‘the principle of local self-government shall be recognised in domestic legislation, and where practicable in the constitution’. Article 3 of this charter provides that ‘local self-government denotes the right and the ability of local authorities, within the limits of the law, to regulate and manage a substantial share of public affairs under their own responsibility and in the interests of the local population’ [17]. Ukraine signed the European Charter of Local Self-Government in 1996, and the Charter entered into force in Ukraine in 1998 [18].

According to the constitution of Ukraine, decentralisation is a process of transferring parts of the functions and powers of the central executive bodies to regional and local self-government bodies [19]. The issue of the Ukrainian decentralisation process was investigated by Vasylieva et al. [20], also the decentralisation reform as a domestic development was noted by Keudel and Huss [21], international support for decentralisation and processes of decentralisation as a tool for the advancement of governance and for conflict management was described by Rabinovych and Gawrich [22]. Indeed, decentralisation of public authority is the process of redistributing competencies between the central and local levels with a shift in the focus of implementation on the ground of pre-defined functions guaranteed by the state.

In 2015, Ukraine adopted the Sustainable Development Strategy ‘Ukraine – 2020’, which provides for the implementation of 62 reforms, including decentralisation [23]. The decentralisation reform involves the creation of a new link in the system of administrative organisation in Ukraine through the introduction of a new administrative-territorial unit – the United Territorial Community (UTC – Hromada). They are formed as a result of the voluntary association of adjacent territorial communities, villages, towns, and cities in accordance with the Law of Ukraine ‘On Voluntary Association of Territorial Communities’ [24].

Current Ukrainian legislation does not define the concept of the Hromada. It indicates that a Hromada includes a voluntary association of residents of several villages, towns, and cities that have a single administrative centre. According to Article 140 of the Constitution of Ukraine, local self-government is the right of a territorial community to independently resolve issues of local importance within the limits of the Constitution and laws of Ukraine. So, a ‘united territorial community – Hromada’ is a set of residents united by permanent residents within a certain village, town, or city, which are independent administrative-territorial units with a single administrative centre.

The powers of territorial communities derive primarily from the Constitution of Ukraine and the Laws of Ukraine's 'On Local Self-Government' and 'On Voluntary Association of Territorial Communities'. In particular, the analysis of Art. 140–143 of the Constitution shows that most issues of local importance are not resolved by Hromadas directly but through local self-government bodies created by them.

Under the decentralisation reform, the Hromadas have gained greater powers, resources, and responsibilities, and legislative changes have increased the range of services that they can provide locally. Therefore, citizens of such Hromadas expect to have convenient and high-quality administrative services from their local authorities. With the support of international donor programmes, centres for the provision of administrative services (TSNAPs) have been created. These are premises where, according to the 'single window' principle, citizens can get the necessary administrative services. International donors and programmes, include the Representation of the European Union in Ukraine, 'U-LEAD with Europe', and USAID.

Regarding the U-LEAD programme, it is worth noting that it is financed by the European Union and its member countries Denmark, Estonia, Germany, Poland, and Sweden. In a project description, U-LEAD's thematic priorities are described as follows: 'It improves the capacities of municipalities to carry out the newly assigned tasks and promotes citizen and private sector engagement in local affairs. U-LEAD provides advice on strengthening local self-government (LSG) and regional development to the national level, improving coordination between different ministries and levels of government' [25].

In Ukraine, there is a three-level administrative-territorial system, where the first place is the regional level divided into oblasts, the second place is the subregional level (districts), and the third place is the basic level – which is divided into administrative-territorial units ('Hromadas'), which consist of cities, urban villages, and villages. Nowadays, there are 1470 Hromadas in Ukraine as a result of the decentralisation reform that shown in the Table 2. The decentralisation processes included the following: administrative services, local budgets, health care, social services, cooperation with municipalities, education, and security.

According to the digitalisation process in this paper, it refers to the integration of digital technologies into various aspects of society

Table 2. The new system of administrative and territorial organisation as of October 7, 2021.

Regional level (Oblast)	Number of basic-level administrative-territorial units ('Hromadas')	Number of administrative-territorial units of the subregional level (districts)
AR Crimea	–	10
Vinnytska	63	6
Volynska	54	4
Dnipropetrovska	86	7
Donetska	66	8
Zhytomyrska	66	4
Zakarpatska	64	6
Zaporizhska	67	5
Ivano-Frankivska	62	6
Kyivska	69	7
Kirovogradska	49	4
Luhanska	37	8
Lvivska	73	7
Mykolaivska	52	4
Odeska	91	7
Poltavska	60	4
Rivnenska	64	4
Sumska	51	5
Ternopilska	55	3
Kharkivska	56	7
Khersonska	49	5
Khmelnytska	60	3
Cherkaska	66	4
Chernivetska	52	3
Chernihivska	57	5
Kyiv city	1	–
Total	1470	136

Based on the source [26].

through the public authorities mainly to transform traditional processes, systems, and activities. About the digitalisation technologies, which are used mainly in the sphere of services such as financial, educational, and public was highlighted by Khadzhyradieva et al. [27].

Digitalisation involves the adaptation of digital technologies in public authorities such as computers, mobile devices, and software applications to enhance efficiency, as well as to make effective services and create new opportunities for innovation and growth. And e-government – is about how government organises itself: its administration, rules, regulations, and frameworks set out to carry out service delivery and to coordinate, communicate, and integrate processes within itself digitally noted by Almarabeh and AbuAli [28], regarding the cybersecurity issues, it plays a key role in the success of e-government programmes [29]. In Ukraine, e-government is a requirement for public administration reform on the one hand, and a key tool in the fight against corruption in government (political and administrative corruption) mentioned by Marysyuk et al. [30].

Importantly, the Ukrainian process of digitalisation in public authorities and local bodies as well began mainly in 2019 with the announcement of the 'Digital State' project, and it is still being implemented. The goal of the project is that all government services will be available online; 20% of services will be provided automatically; there will be one online form to fill out to get the package services for any life situation. As part of the project, 14 test services have already been launched: electronic office, mobile app, e-Baby, passport with TIN, child registration online, e-pension, SmartID, MobileID, digital citizenship certificate, e-residency, developer's office, bank account for business online, electronic elections, and ID card with electronic signature. 'The state in a smartphone' is available now in the 'Diia' application, and all online services in the Diia – Government services online, which are divided into two groups for citizens and business.

According to the countries in Europe with the highest E-Government Development Index (EGDI) values, Ukraine in 2022 is in the 46th rank, which means that it improved compared to position 69 in 2020 [31]. This growth is explained by the Ukrainian application Diia as a digital passport and portal where citizens can get a service using this application or site as all data is attached to the person and it is available in digital form.

When the full-scale invasion began, local authorities were decentralised, but not all of them, as the reform was still in the process of implementation, and digitalisation had started almost at the same time and was actively developing, and still it was needed the digital transformation specialists in the regions, that needs time and sources. Additionally, when there is a change in the organisation, everything is in a situation of uncertainty, and in a war situation it increases.

4. Cyber Attacks Definitions

There is no unified definition of the term ‘cyber attacks’ in the scientific literature. Therefore, in this article, cyber attacks are understood as actions carried out by cyber actors in cyberspace on special targets which lead to violations of (i) privacy, (ii) information availability, (iii) critical infrastructures, and (iv) psychological effects on minds, i.e., confusion about what constitutes the truth, and on the mental state of citizens, such as anxiety and panic.

As mentioned by Michael Kenney (2015) cyber attacks belong to the same metaphorical class or ‘genus’ of events as cyber-war, ‘hacktivism’ and terrorists’ use of the internet [4].

Cyber attacks can be understood as ‘the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population’ [32]. They ‘pose complex problems that reach into new areas for national security and public policy’. Data and information are getting more vulnerable in this situation of cyber attack, especially if the level of protection is low and local authorities pay little attention to this field.

Inspired by Plotnek et al. and based on the definitions proposed by Al Mazari et al. above the following Figure 1 presents a formation of dimensions which cyber attacks include.

Cyber attacks can be malicious (e.g., trojan horses, computer worms, and sabotage attacks) or unintentional (e.g., incorrect

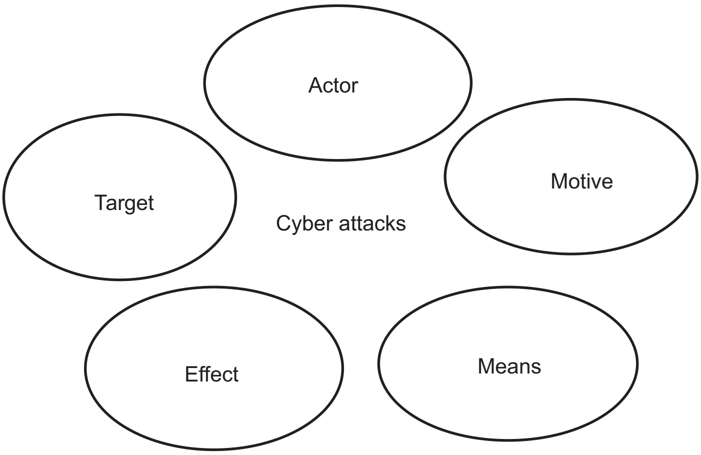


Figure 1. Dimensions of cyber attacks.

software updates, erroneous protocols, or unwanted network connections). The motivation for malicious attacks may among others arise from terrorism, geopolitics, or criminality. According to Stambaugh [33] terrorist cyber attacks are considered 'the premeditated, politically motivated attack against information systems, computer programs, and data to deny service or acquire information with the intent to disrupt the political, social, or physical infrastructure of a target resulting in violence against noncombatants. The attacks are perpetrated by subnational groups or clandestine agents who use information warfare tactics to achieve the traditional terrorist goals and objectives of engendering public fear and disorientation through disruption of services and random or massive destruction of life or property'.

Cyber attacks represent complex problems whose effects reach into new areas for national security and public policy [34]. As mentioned above, cyber actors can use computer network tools to shut down critical national infrastructures (such as energy, transportation, and government operations) or to coerce or intimidate a government or civilian population.

After considering all the keywords related to cyber attacks, a simplified graphical illustration of the dimensions of cyber attacks was compiled with a view to Ukrainian municipalities (see Figure 2).

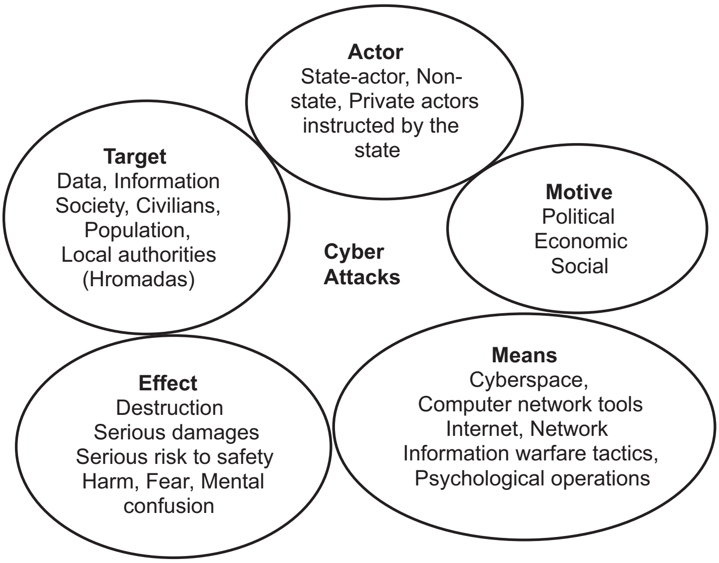

Actor
State-actor, Non-state, Private actors instructed by the state
Target
Data, Information Society, Civilians, Population, Local authorities (Hromadas)
Cyber Attacks
Motive
Political
Economic
Social
Effect
Destruction
Serious damages
Serious risk to safety
Harm, Fear, Mental confusion
Means
Cyberspace,
Computer network tools
Internet, Network
Information warfare tactics,
Psychological operations

Figure 2. Dimensions of cyber attacks in Ukrainian municipalities.

The key features of cyber attacks can be segmented and contrasted by the relevant components Al Mazari et al. (2018) based on it created dimensions of cyber attacks in Ukrainian municipalities using five key components:

- **Target:** Data, Information society, Civilians, Population, and Local authorities (Hromadas)
- **Motive:** Political, Economic, and Social
- **Means:** Cyberspace, Computer network tools, Internet, Network, Information warfare tactics, and Psychological operations
- **Effect:** Destruction, Serious damages, Serious risk to safety, Harm, Fear, and Mental confusion
- **Actor:** State-actor, Non-state, and Private actors instructed by the state

During analysis, however, it was noted that more recent literature emphasises aspects relating to motive threat investigated by Plotnek and Slay [35], which led to the discovery of a vital gap regarding the threat actor in the cyber-attack dimensions that proposed here.

To analyse the municipalities' protection against potential cyber attacks, the Swiss Cheese Model can be strengthened, which was developed by Reason et al. [36]. The main idea of the model is to explain why accidents and failures sometimes occur even when multiple layers of defence are in place. The model has since been applied to various fields, including aviation, healthcare, and cybersecurity. According to James T. Reason, each slice of Swiss cheese is full of holes and the size, and number of holes will vary from one slice to another. In this model, a slice of Swiss cheese is symbolic of a given measure taken to minimise risk. Each slice of cheese can be thought of as a line of defence level against accidents level. In cybersecurity, this model can be effective to visualise controls and defences that public authorities or municipalities have in place to protect themselves from cyber threats.

These cheese holes can be used by attackers to compromise an organisation's defences. However, the model (Figure 3) also suggests that the chances of an attacker successfully breaching an organisation's defences are greatly reduced if there are multiple layers of protection, as an attacker would need to find a vulnerability in each layer to successfully exploit it. One of the key benefits of the Swiss cheese model is that it encourages organisations to take a holistic approach to cybersecurity and not just focus on one control or protection mechanism. The model encourages organisations

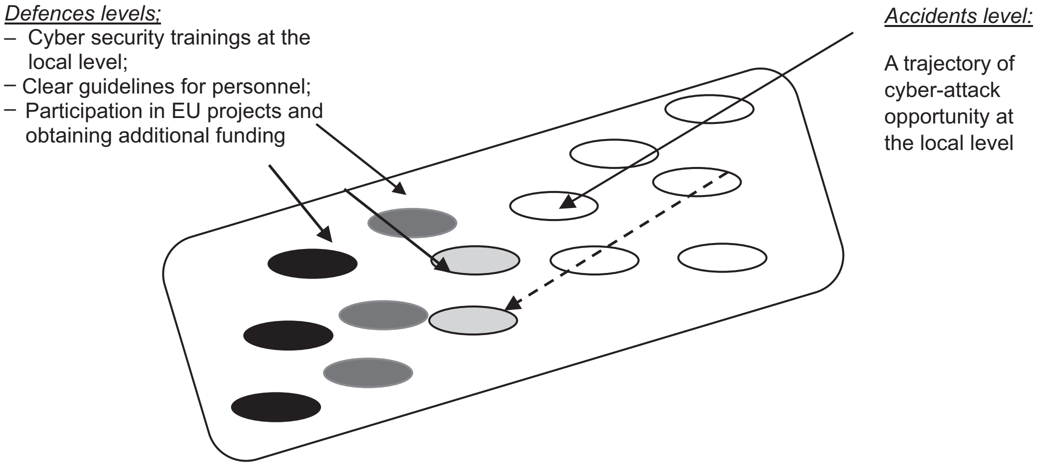

Defences levels;
– Cyber security trainings at the local level;
– Clear guidelines for personnel;
– Participation in EU projects and obtaining additional funding
Accidents level:
A trajectory of cyber-attack opportunity at the local level

Figure 3. Cyber attacks vulnerabilities at the local level with potential accidents and defences levels based on the Swiss cheese model.

to consider the entire system of controls and protections they have in place and how they can be strengthened.

For example, if employees of the local authorities have listened to training on preventing phishing attacks, not to open unknown links and basic ideas of hygiene on the internet, then one of these slice-levels of protection according to this model is already more protected. However, if employees are not trained in how to detect and prevent phishing attacks, an organisation can still be vulnerable to cyber attacks through this 'hole' in its defences. Another slice that can prevent cyber attacks is the developed guidelines for cybersecurity at the local level.

5. Cyber attack cases in local authorities in Ukraine during 2022–2023

Massive cyber attacks were held on the governmental websites during January 2022 before the full-scale invasion of Ukraine. There were a lot of cyber attacks on the websites of local authorities in Ukraine in spring 2022. According to the State Service of Special Communications and Information Protection of Ukraine Report, cyber attacks took place in different sectors during 2022–2023, but governmental and local authorities were in second place, as shown in Figure 4.

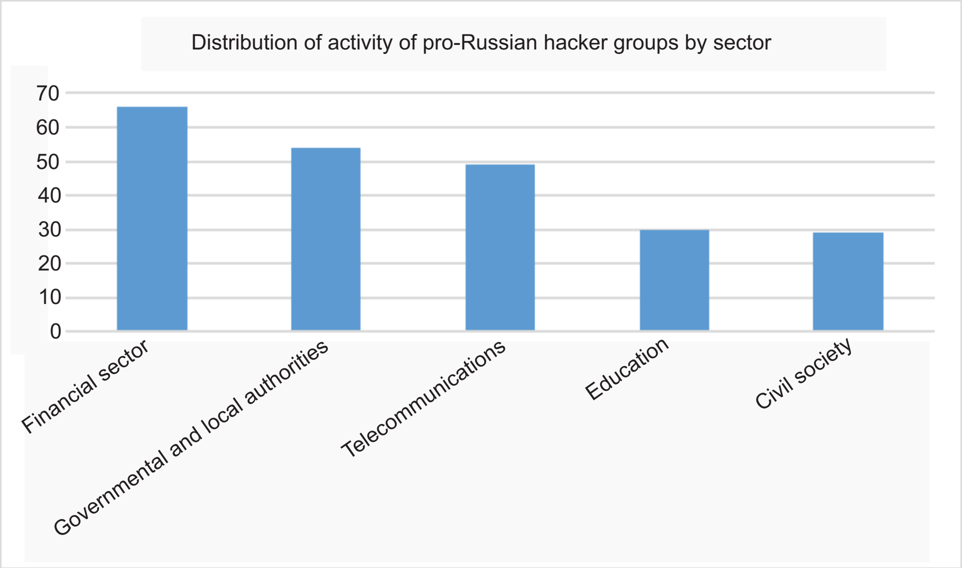


Figure 4. Distribution of activity of pro-Russian hacker groups by sector based on the SSSCIPU data report [13].

Indeed, as mentioned by the manager of the Volyn regional civil administration, the websites of the communities were hacked in the Volyn region on March 3, 2022, and the representatives of the administration of the affected communities asked the citizens not to react and not to spread misinformation.

The spokeswoman of the Security Service of Ukraine in the Zhytomyr region said that a cyber attack was committed on the websites of the community in the Korosten district.

In the same period, the head of the Vinnytsia regional administration, Serhii Borzov, noted that cyber attacks were carried out on the websites of regional state administrations and communities. Borzov also noted that computer algorithms have learned to ‘revive’ photos, synthesise a person’s voice, and replace a face in a certain video.

The press service of the Bereziv city council of the Odesa region reported that the occupiers had hacked the websites of all communities in the Odesa region and published information about the alleged ‘surrender of Ukraine’. This was a fake [37]. All these examples from March 2022 were similar in content. Cyber attacks were used to affect the psychological and mental state of the population in the communities.

In April 2023, there was a cyber attack on the official information resources of the Uman community in the Cherkasy region [38]. The rural and town websites are not available to users and administrators themselves. According to IT engineer Oleksandr Lampika:

‘Hackers carried out a DDoS attack on the corresponding server, this is a huge number of connections at the same time, and it “went down” a bit. Oleksandr believes that this attack will not bring any benefit to the enemies, except for our temporary inconveniences. These DDoS attacks are the same as bombing fields they just do damage. Our specialists know very well what to do in such cases, everything will be repaired on the servers and the sites will work again. It takes a little time.’

Indeed, some of the representatives of Ukrainian local authorities mentioned about cases facing cyber attacks during the full-scale invasion of Ukraine. As noted, the IT specialist of the Western community:

> The first cyber attack on our community site took place in 2022, after the full-scale war began. The site was down for some time, our technical website developer reacted immediately, and the site resumed operation the next day, so, I would like to note that citizens had access to the site quickly. The second time when we faced the cyber attack it happened in the spring of 2023 and again it lasted up to one day, even several hours and then our technical support restored access to the site.

Thus, this destruction effect spreads anxiety, fear, or mental confusion situations inside society, especially with the full-scale invasion.

According to the research of the Ministry of Digital Transformation of Ukraine, the digital skills of Ukrainians and the level of digital security in 2023, where cybersecurity policies of surveyed Ukrainians do not have policies on cybersecurity and/or cyber hygiene at the workplace 36%; and 26% answered there is no effective protection of confidential information [39]. Hence, this shows the importance of strengthening resilience in the cybersecurity field in the country and in local authorities especially.

6. EU support

Before the full-scale invasion, the EU supported Ukraine in countering cyber attacks by launching a cyber dialogue between the EU and Ukraine in June 2021, strengthening the operational capacity of the country's telecommunications services and the fight against disinformation. In addition, at the request of the Ukrainian government, the EU activated the PESCO Cyber Rapid Response Teams in February 2022 for the first time in an operational context [40]. In February 2022, the US Cyber Command team assisted cyber rapid response teams in the search for active threats. In March 2022, Ukraine became a contributing member of NATO Joint Cyber Defense Center of Excellence. The European Center of Excellence for Countering Hybrid Threats as well strengthened its cooperation. Also, in March 2022, the EU Parliament called for immediate and full implementation of all decisions that would increase the EU's contribution to strengthening Ukraine's defence capacities, including cybersecurity.

On the local level, the main responsibility for the support from the EU to Ukrainian local authorities provides the U-Lead programme, which includes policy and legal advice to local levels, training support, and consultation. Hence, regarding the interviews with the questions about the EU support for the local authorities that facing cyber attacks during 2022–2024, some of the representatives answered that they cooperate with the U-Lead programme. As mentioned, the IT specialist of the Western community:

> Our community cooperated with the U-LEAD program, they helped us with the opening of the Administrative Services Center (TSNAP), and we also received computer equipment for the TSNAP from them.

Another example of cooperation with the U-Lead programme mentioned the decision maker from the central region community:

> Among EU projects, we cooperated with U-Lead when we opened the Administrative Services Centre (TSNAP). Also, we take part in all training, including cyber security.

The politician representative from one of the eastern communities noted:

> We cooperated with U-Lead programme as part of the opening of TsNAP in our community.

Furthermore, the East Europe Foundation as a non-profit charitable organisation supports local authorities in Ukraine with the aim to build a strong, active civil society, effective, democratic government at all levels, and institutional development among community organisations and government agencies. Moreover, it provides cybersecurity training, digital for local authorities together with the platform zlozumilo, and some experts have indicated participation in these trainings. For example, an IT specialist of the southern community noted:

> We cooperate a lot with the U-Lead program, and we had support with openning our TSNAP. And we also, participate in the cyber security trainings that conducted by the Eastern European Foundation.

While five experts noted that they lack IT professionals in general to implement digitalisation and also to be aware of cyber incidents. Particularly, one of them from the central region of Ukraine mentioned:

> In our community, there is only one IT specialist who is responsible for whole digital and cyber processes.

At the same time, the decision maker from the northern region highlighted about physical damage in the community and their priority for rebuilding the houses of citizens, which were damaged in the conditions of the full-scale invasion of Russia into Ukraine:

> We have a lot of destroyed houses, citizens are actively using the Diia digital application, recording the damage to their buildings of the war. And in this case, digitalization is very helpful, in terms of processing and recording cases, which is a priority at the moment.

Despite the EU's support to Ukrainian local authorities, which are facing cyberattacks, mentioned by experts, there are certain challenges associated with this assistance. These challenges include a lack of personnel, lack of funding, complex application procedures for the EU projects, lack of coordination, and technical capacity limitations.

Where underfunding is interdependent with understaffing in the digital field, as funding is needed to increase staffing. Regarding the complex application procedures as to gain the EU funding for cybersecurity projects may be excluded by complex application procedures, administrative requirements, and eligibility criteria and local authorities' representatives would need training for this. According to the challenge of as lack of coordination, it may create insufficient processes of communication between Ukrainian local authorities, national government agencies, and EU institutions, leading to fragmented approaches to cybersecurity governance and implementation. And the lack of a single strategy and coordination mechanism can undermine the effectiveness of EU support efforts and lead to duplication of efforts, and new approaches such as boundary spanning can be the response to this challenge [41]. Concerning technical capacity limitations – Ukrainian local authorities may lack the technical resources and institutional capacity to effectively utilise EU support for cybersecurity initiatives. As mentioned by the decision maker from the northern region in Ukraine:

> The community received technical support from the EU in the form of computers, but their technical capacity.

These and other challenges may be explored in future publications. There are some challenges with cyber attacks and cybersecurity described in scientific publications in the public administration field, and to a lesser extent, those related to the field of local government. Overall, cybersecurity needs to be viewed as a shared responsibility rather than being relegated to IT teams, as highlighted by Brumfield [42], especially when Ukraine has a full-scale Russian invasion of Ukraine and about the war conditions noted Guchua and Zedelashvili [43] the biggest problem is that aggressive states, terrorist organisations, non-state groups, large corporations, etc. are mostly involved in the virtual war as well. The importance of the creation the cybersecurity guidance for public managers in developing and implementing strategies was mentioned by Wirtz and Weyerer [44], and Norris et al. [45, 46] found from the conducted survey in the US that among state and local governments, the two top challenges to achieving high levels of cybersecurity were a lack of skilled personnel and lack of funding. In addition, about the lack of funding at the local level and about the crucial situation to disseminate knowledge about available sources of funding for expenses on cybersecurity, and about good practices in this area, as well as to simplify the rules for using external sources of funding, including EU funds it was emphasised by Choodakowska et al. [47]. As a technical threat, Whitehead et al. [48], indicates that includes weak technical capacities, incompatible technologies, equipment failures, and software failures.

7. Conclusions

The creation of cooperation networks of partnerships with neighbouring communities to share knowledge and cases of cyber attacks, as well as sharing experience in writing and submitting EU projects will improve integration processes to the EU and strengthen resilience at the local level. A proposed Swiss cheese model for analysing the vulnerabilities of potential cyber attacks in communities and minimising risks to strengthen the resilience of local governments. Furthermore, examining the dimensions of cyber attacks at the local level that proposed in the article such as actor, target, motive, effect, and means would build up better cyber protection.

Consolidating existing cybersecurity training programmes onto a single platform and providing comprehensive information about them for local authorities. Considering that cyber attacks can cause harm to citizens and their data, therefore, state authorities should carry out random audits to identify any irregularities in this regard. Engage veterans, who are ready to work in the cybersecurity field that can be as win-win situation in the country, the minds of veterans will be useful to local authorities, and they will be socially active. Also, active leadership positions in the municipalities may deepen the driving digital transformation at the local level and public administration in general. Ukraine's participation in the Digital Europe programme will provide deeper support for projects on cybersecurity and advanced digital skills and will also ensure the widespread use of digital technologies in the municipalities, including through digital innovation centres. Additionally, the development of training programmes with the aim to enhance the complex application procedures skills of local authority personnel for EU project procedures that would improve the acquisition of possible projects and accordingly, funding.

Acknowledgements

Special thanks to the Scholar at Risk Programme in Norway and the Department of Political Science and Management at the University of Agder for providing the scholarship and the opportunity to conduct this research. The author is grateful to respondents who agreed to be interviewed particularly amidst the challenging wartime circumstances in Ukraine. Also, the author appreciates the generous input of the article reviewers.

References

[1] A. Frandell, M. Feeney, "Cybersecurity threats in local government: A sociotechnical perspective," *The American Review of Public Administration*, vol. 52, no. 8, pp. 558–572, 2022, doi: 10.1177/02750740221125432.

[2] A. Ibrahim, C. Valli, I. McAteer, I. Chaudhry, “A security review of local government using NIST CSF: A case study,” *The Journal of Supercomputing*, vol. 74, pp. 5171– 5186, 2018, doi: 10.1007/s11227-018-2479-2.

[3] W. Hatcher, W.L. Meares, J. Heslen, “The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices,” *Journal of Cyber Policy*, vol. 5, no. 2, pp. 302–325, 2020, doi: 10.1080/23738871.2020.1792956.

[4] M. Kenney, “Cyber-terrorism in a post-Stuxnet world,” *Orbis*, vol. 59, no. 1, pp. 111–128, 2015, doi: 10.1016/j.orbis.2014.11.009.

[5] N. Kostyuk, E. Gartzke, “Why cyber dogs have yet to bark loudly in Russia’s invasion of Ukraine (Summer 2022),” *Texas National Security Review*. [Online]. Available: https://tnsr.org/wp-content/uploads/2022/06/TNSR-Journal-Vol-5-Issue-3-Kostyuk-Gartzke.pdf. [Accessed: Jan. 12, 2024].

[6] O. Evsyukova, “Political digitalization for Ukrainian society–challenges for cyber security,” *Cybersecurity and Law*, vol. 5, no. 1, pp. 139–144, 2021, doi: 10.35467/cal/142199.

[7] A. Pintsch, “Decentralization in Ukraine and bottom-up European integration,” in *Decentralization, Regional Diversity, and Conflict: The Case of Ukraine*, H. Shelest, M. Rabinovych, Eds., Palgrave Macmillan Cham, 2020, pp. 339–363.

[8] V.P. Hordiienko, M.L. Onishchenko, I.S. Malyonkina. (2019). *Foreign experience of decentralization of public power and the possibility of its transformation in Ukraine.* [В. П. Гордієнко, М. Л. Оніщенко, І. С. Мальонкіна. (2019). *Зарубіжний досвід децентралізації публічної влади та можливості його трансформації в Україні*]. [Online]. Available: https://essuir.sumdu.edu.ua/handle/123456789/76912. [Accessed: Jan. 12, 2024].

[9] D.O. Lukin, V.P. Gordienko, G.O. Myroshnychenko, *Fundamentals of Power Decentralization: Methodological Recommendations*, Council of Young Scientists, Sumy, 2015. [Д.О. Лукін, В.П. Гордієнко, Г.О. Мирошниченко, *Основи децентралізації влади: методичні рекомендації*, Рада молодих вчених, Суми, 2015]. [Online]. Available: https://issuu.com/34462/docs. [Accessed: Jan. 12, 2024].

[10] H. Wagenaar, *Meaning in Action: Interpretation and Dialogue in Policy Analysis*, London and New York: Routledge, 2014.

[11] C. Dyer, P. Rose, “Decentralisation for educational development? An editorial introduction,” *Compare: A Journal of Comparative and International Education*, vol. 35, no. 2, pp. 105–113, 2005, doi: 10.1080/03057920500129809.

[12] O. Mikuš, M. Kukoč, M. Jež Rogelj, “The coherence of common policies of the EU in territorial cohesion: A neverending discourse? A review,” *Agricultural Economics*, vol. 65, pp. 143–149, 2019, doi: 10.17221/229/2018-AGRICECON.

[13] State Service of Special Communications and Information Protection of Ukraine Report. (Jul. 10, 2022). *Report for Q3 2022*. [Online]. Available: https://scpc.gov.ua/en/articles/163. [Accessed: Jan. 12, 2024].

[14] Microsoft Threat Intelligence. (2023). *Microsoft Digital Defence Report. Building and improving cyber resilience*. [Online]. Available: https://microsoft.com/mddr. [Accessed: Dec. 22, 2023].

[15] Cybersecurity Tech Accord. (2023). *Building a voice for peace and security online. The cybersecurity tech accord’s first five years*. [Online]. Available: www.cybertechaccord.org. [Accessed: Dec. 22, 2023].

[16] Council of Europe. (Sep. 01, 1988). *Chart of Signatures and Ratifications of Treaty 122 of the European Charter of Local Self-Government.* [Online]. Available: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=122. [Accessed: Dec. 18, 2023].

[17] Council of Europe. (Oct. 15, 1985). *The European Charter of Local Self-Government.* [Online]. Available: https://rm.coe.int/168007a088. [Accessed: Dec. 18, 2023].

[18] Law of Ukraine On Ratification of the European Charter of Local Self-Government of July 15, 1997 [Закон України Про ратифікацію Європейської хартії місцевого самоврядування від 15 липня 1997 року]. [Online]. Available: https://zakon.rada.gov.ua/laws/show/452/97-%D0%B2%D1%80#Text. [Accessed: Dec. 18, 2023].

[19] Constitution of Ukraine [Конституція України]. [Online]. Available: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text. [Accessed: Dec. 18, 2023].

[20] N.V. Vasylieva, O.I. Vasylieva, S.M. Prylipko, S.V. Kapitanets, O.V. Fatkhutdinova, "Approaches to the formation of public administration in the context of decentralization reform in Ukraine," *Cuestiones Politicas*, vol 38, no. 66, pp. 301–320, 2020, doi: 10.46398/cuestpol.38e.19.

[21] O. Keudel, O. Huss, "Polycentric governance in practice: The case of Ukraine's decentralised crisis response during the Russo-Ukrainian war," *Journal of Public Finance and Public Choice*, vol. 39, no. 1, pp. 10–35, 2024, doi: 10.1332/25156918Y2023D000000002.

[22] M. Rabinovych, A. Gawrich, "The conflict in Eastern Ukraine and international support for the decentralization reform (2014–2022): Theory-guided observations," *East European Politics and Societies*, vol. 37, no. 3, pp. 1036–1058, 2023, doi: 10.1177/08883254221139841.

[23] Decree of the President of Ukraine, *On the Sustainable Development Strategy 'Ukraine – 2020'* [Указ Президента України, *Про Стратегію сталого розвитку 'Україна – 2020'*], Jan. 12, 2015. [Online]. Available: https://zakon.rada.gov.ua/laws/show/5/2015#Text. [Accessed: Dec. 16, 2023].

[24] Law of Ukraine, *On Voluntary Unification of Territorial Communities* [Закон України, *Про добровільне об'єднання територіальних громад*], 2015. [Online]. Available: https://zakon.rada.gov.ua/laws/show/157-19#Text. [Accessed: Dec. 20, 2023].

[25] Ministry for Communities and Territories Development of Ukraine (MinRegion). (2022). *U-LEAD with Europe's contribution to a transparent, accountable and responsive multi-level governance in Ukraine, February 2022*. [Online]. Available: https://www.giz.de/de/downloads/giz2022-en-u-lead-four-pager.pdf. [Accessed: Jan. 04, 2024].

[26] *Monitoring of the reform of local self-government and territorial organization of power of the Ministry of Development of Communities and Territories of Ukraine as of October 7, 2021* [*Моніторинг реформи місцевого самоврядування та територіальної організації влади Міністерства розвитку громад та територій України станом на 07 жовтня 2021 року*], Apr. 1, 2024. [Online]. Available: https://www.minregion.gov.ua/wp-content/uploads/2019/01/monitoryng-reformy-misczevogo-samovryaduvannya-ta-terytorialnoyi-organizacziyi-vlady-stanom-na-1-zhovtnya-2021r..pdf. [Accessed: Jan. 04, 2024].

[27] S. Khadzhyradieva, T. Docsenko, M. Sitsinska, Y. Baiun, Y. Pukir, "Prerequisites for process management implementation in the public administration of

Ukraine," *International Journal of Criminology and Sociology*, vol. 9, pp. 2825–2833, 2020, doi: 10.6000/1929-4409.2020.09.346.

[28] T. Almarabeh, A. AbuAli, "A general framework for e-government: Definition maturity challenges, opportunities, and success," *European Journal of Scientific Research*, vol. 39, no. 1, pp. 29–42, 2010.

[29] J.P. Kesan, L. Zhang, "An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 582-596, 2019, doi: 10.1109/TETC.2019.2915098.

[30] K.B. Marysyuk, I.O. Tomchuk, M.D. Denysovskyi, I.O. Geletska, B.V. Khutornyi, "Diia. Digital state and E-government practices as anti-corruption tools in Ukraine Institutions," *WSEAS Transactions on Environment and Development,* vol. 17, pp. 885-897, 2021, doi: 10.37394/232015.2021.17.83.

[31] United Nations. (2022). *E-government Development Index*, [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine. [Accessed: Dec. 16, 2023].

[32] J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, Washington, DC, 2002.

[33] H. Stambaugh, *Electronic crime needs assessment for state and local law enforcement*, US Department of Justice, Office of Justice Programs, National Institute of Justice, 2001.

[34] M.S. Mahmoud, M.M. Hamdan, U.A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019, doi: 10.1016/j.neucom.2019.01.099.

[35] J.J. Plotnek, J. Slay, "Cyber terrorism: A homogenized taxonomy and definition," *Computers and Security*, vol. 102, 2021, doi: 10.1016/j.cose.2020.102145.

[36] J. Reason, E. Hollnagel, J. Paries, "Revisiting the Swiss cheese model of accidents," *Journal of Clinical Engineering*, vol. 27, no. 4, pp. 110–115, 2006.

[37] Dzerkalo Tuzhnya. (Mar. 3, 2022). *In five oblasts, the websites of local authorities were hacked: The Russian Federation spreads fakes on the.* [Дзеркало Тижня. (3 березня 2022). *В п›ятьох областях зламано сайти місцевої влади: РФ розповсюджує на них фейки*]. [Online]. Available: https://zn.ua/ukr/UKRAINE/u-volinskij-ta-vinnitskij-oblastjakh-zlamano-sajti-mistsevoji-vladi-rf-rozpovsjudzhuje-na-nikh-fejki.html. [Accessed: Jan. 12, 2024].

[38] Uman News. (May 25, 2023). *Virtual damage for defeats at the front: a cyber attack continues on the official websites of hromadas of the Uman district*. [Online]. Available: https://umannews.city/articles/289379/virtualna-shkoda-za-porazki-na-fronti-trivaye-kiberataka-na-oficijni-sajti-gromad-umanskogo-rajonu. [Accessed: Jan. 14, 2024].

[39] Ministry of Digital Transformation of Ukraine. (2023). *Research on digital skills in Ukraine*. [Міністерство цифрової трансформації України. (2023). *Дослідження цифрової грамотності в Україні*]. [Online]. Available: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf. [Accessed: Jan. 04, 2024].

[40] European Parliamentary Research Service. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. [Accessed: Jan. 03, 2024].

[41] A. C. Lindholst, D. O. Torjesen, "Special issue introduction: Boundary spanning in the age of collaborative governance – Insights from Nordic local governments," *Scandinavian Journal of Public Administration*, vol. 28, no. 1, pp. 1–10, 2024, doi: 10.58235/sjpa.2024.22522.

[42] C. Brumfield. (May 06, 2022). *Why local governments are a hot target for cyber-attacks*. [Online]. Available: https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-forcyberattacks.html. [Accessed: Nov. 11, 2021].

[43] A. Guchua, T. Zedelashvili, "Challenges arising from cyber security in the dimension of modern global security (on the example of the Russia-Ukraine war)," *Eastern Review*, vol. 11, no. 2, pp. 79-88, doi: 10.18778/1427-9657.11.18.

[44] B. W. Wirtz, J. C. Weyerer, "Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats," *International Journal of Public Administration*, vol. 40, no. 13, pp. 1085–1100, 2017, doi: 10.1080/01900692.2016.1242614.

[45] D.F. Norris, L. Mateczun, A. Joshi, T. Finin, "Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity," *Public Administration Review*, vol. 79, no. 6, pp. 895–904, 2019, doi: 10.1111/puar.13028.

[46] D.F. Norris, L. Mateczun, A. Joshi, T. Finin, "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity," *Journal of Urban Affairs*, vol. 43, no. 8, pp. 1173–1195, 2020, doi: 10.1080/07352166.2020.1727295.

[47] A. Choodakowska, S. Kańduła, J. Przybylska, "Cybersecurity in the local government sector in Poland: More work needs to be done," *Lex Localis*, vol. 20, no. 1, pp. 161–192, 2022, doi: 10.4335/20.1.161-192(2022).

[48] D.E. Whitehead, K. Owens, D. Gammel, J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies." 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 2017, pp. 1–8, doi: 10.1109/CPRE.2017.8090056.

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Methodology of Quantitative Assessment of Network Cyber Threats Using a Risk-Based Approach

Artem Zhylin | The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, The Cybersecurity and Application of Information Systems and Technology Academic Department at the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" | ORCID: 0000-0002-4959-612X

Hanna Holych | The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine | ORCID: 0000-0003-0849-5127

Abstract

The methodology of a quantitative assessment of organisation's network cyber threats was developed in order to quantitatively assess and compare the cybersecurity threat landscape in conditions of limited data while applying the risk-oriented approach. It can be used either for assessing the level of network cyber threats of a particular organisation (as a quantitative measure of the criticality of cyber threats that are detected within the organisation's network) or for comparing the level of network cyber threats of several organisations during the same or different time periods, giving grounds for supporting the process of making managerial decisions regarding the organisation's cybersecurity strategy. The proposed scheme of the algorithm can be used to automate the calculation process. The assessment of network cyber threats that are considered in the article is not a full-fledged measure of the cyber risk because the methodology was developed considering the common circumstances of the deficiency of the risk context data. Nevertheless, the results of the methodology implementation partially reflect the overall level of the

Received: 13.02.2024

Accepted: 27.04.2024

Published: 15.07.2024

Cite this article as:
A. Zhylin, H. Holych "Methodology of quantitative assessment of network cyber threats using a risk-based approach," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190345

Corresponding author:
Hanna Holych, State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine; E-mail: h.holych@cip.gov.ua;
0000-0003-0849-5127

organisation's cyber risk and are expected to be used in the case when the full-featured proper cyber threats assessment can't be organised for some reason.

Keywords

cyber risk, network cyber threats, quantitative assessment, risk-oriented approach, network cybersecurity domain, cyber threat landscape

1. Introduction

Assessment is a process that allows one to determine whether the implemented measures provide the expected impact and therefore contributes to establishing cause-and-effect relationships between actions and results. One of the fundamental issues in the field of cybersecurity is the assessment of the effectiveness (the degree of completeness of the realised impact) of the implemented cyber defence measures (countermeasures against cyber threats) that is conducted to check the validity and usefulness of such measures while mitigating cyber risks, as well as for the further adjustment of the organisation's general cybersecurity strategy. In this context, the determination of the organisation's approach to the assessment of cyber threats as well as their identification and analysis are among the main tasks of the risk management process.

Cyber threat assessment is an actual and popular area of scientific research because both the subjective and objective multivariate interpretation of the risk concept itself creates prerequisites for the absence of a uniform approach to its assessment and defining the main factors of direct influence. As of today, the organisation of the process of cyber threat assessment in conditions of limited contextual information and data (resulting in the inaccuracy of such an assessment), the determination of typical cyber threat characteristics that can be used during cyber threat assessment in conditions of such limitations, the instability of cyber threat landscape (resulting in the need for periodic risk factors (indicators) revision in order to maintain the relevance of such assessment) are among the typical problems in this field.

Common ways to solve such problems are the adaptation of popular methodologies and specific methods of cyber threat assessment (which are almost always used not separately, but in the context of risk definition as a more complex concept) and the creation of individual adapted methodologies or methods of the cyber threat score formation, that is the topic of this work.

2. Theoretical Background

2.1. Literature Review

Currently, there is a research gap related to conducting cyber threat assessments based on network traffic, as most studies focus on cyber risk assessment, which is a more complex and comprehensive topic. More than that, according to the analysis of popular and scientific publications on the topic of cyber threat assessment based on network traffic, such assessments are not conducted solely using the indicators derived from network traffic analysis in any of the reviewed works. This is primarily because network traffic can be considered one of multiple data sources for such assessments [1–4], but a cyber threat assessment is a more complex process in general. At the same time, the need for the formation of quantitative indicators, even with limited resources and data [5], is confirmed by the active implementation of such indicators by well-known cybersecurity vendors [6–9] for making managerial decisions.

An explanation of the method of conducting cyber threat assessment based on indicators determined from the network traffic analysis results in combination with the data about vulnerabilities of organisation's assets is given in [10]. Research on the development of a methodology for forming a quantitative score representing the network security situation that is based on attack prediction algorithms is also quite common, for example, Hu *et al.* [11].

Publications related to conducting cyber threat assessment that is not based on network traffic (but in a related context) were also considered during the analysis [12–16]. They helped to more accurately interpret the theoretical interdependence of cybersecurity, cyber risk, cyber threat, and cyber defence indicators, the values of which are often determined or calculated based on the expression of one through the other.

In particular, the methodology [12] describes the dependence of the nature of a cyber threat on indicators of the state of society relations and confirms the relationship between the cyber threat and cybersecurity levels in such a way that the cyber threat level is a criterion for assessing the cybersecurity level. It is also specified that the criterion for assessing the cyber threat level should be mainly based on the nature of the cyber threats and requires the consideration of their scale. Taking into account that organisations' countermeasures against cyber threats of various risk levels differ in the level of cyber attack neutralisation it can be concluded that the level of cyber attack neutralisation (cyber defence indicator) can be considered a criterion for assessing the cyber threat level.

A method for evaluating the effectiveness of measures aimed at ensuring the cybersecurity level of organisations' critical information infrastructure objects is proposed by Pyskun *et al*. [13]. While evaluating the effectiveness (along with the cybersecurity, system functional capacity, and cyber resilience indicators), the cyber risk probability indicator is proposed to be taken into account, which is determined as a combination of the cyber attack probability (that, in turn, depends on the cyber defence level) and its potential impact (amount of possible damage). Also, the criteria for assessing the cyber risk probability, cyber defence, potential impact, and the cyber attack probability are proposed with generalised recommendations on how to determine the levels by calculating the scores (without specifying the method of establishing the unambiguous correspondence of the calculated scores to specific criteria). On the one hand, such an approach makes the methodology more multi-purpose due to the lack of dependence on specific methods of calculating the scores, but on the other hand, it creates grounds for doubting the correctness of the correspondence of the calculated scores to specific criteria due to the same non-determinism of the methods of scores calculation and the lack of a described verification mechanism. In addition, this non-determinism has several levels of impact – firstly, on determining the correspondence with the criteria for the cyber attack probability and evaluating the amount of damage, then on the resulting cyber risk probability score.

In summary, the analysis of recent research publications confirms:

- the functional dependence between cyber security, cyber risk, cyber threats, and cyber defence indicators, which is relevant for understanding the applicability of the proposed approach to network cyber threat assessment in the context of determining its relationship with the other indicators. At the same time, based on the generally accepted functional dependence definition, the value of one indicator (independent or input) affects the value of another indicator (dependent or output). In our case, the definition of dependent and independent indicators is not static but varies according to the problem statement (definition of the main goals and objectives of the research, that must be completed in order to achieve these goals) and the available input data, which are the basis for further calculations.

- the need to define an unambiguous approach for the realisation of every sequential stage of the assessment methodology, or to apply such a level of generalisation in relation to possible approaches that would not create prerequisites for doubts about the correctness of the results obtained at different stages and at the same time would allow a certain level of abstraction (i.e., with the possibility of flexible approach adaptation depending on individual factors).

2.2. Discussion of Common Cyber Risk Factors

Cyber threats, vulnerabilities, impact, likelihood, and predisposing conditions are typical cyber risk factors (according to [17–20]). Cyber risk factors can be decomposed in greater detail (e.g., cyber threats decomposed into cyber threat sources and cyber threat events) before conducting a cyber risk assessment to take into account a greater number of relevant attributes, which, in turn, contribute to increasing the objectivity of such an assessment. Therefore, cyber risk factors are characteristics used in cyber risk models as inputs to the cyber risk assessment process.

Figure 1 represents the cyber risk model based on the typical factors that are used in the work.

Taking into consideration that network cyber threat events form the only data source for the assessment, **it is more appropriate to consider cyber threat (rather than cyber risk) assessment** due to the lack of metrics that could define important cyber risk factors (such as vulnerabilities and predisposing conditions). The terms ‘cyber risk assessment’ and ‘cyber threat assessment’ are often used interchangeably, but in fact, they refer to distinct processes. While both assessments complement each other and are essential components of a robust cybersecurity strategy, they

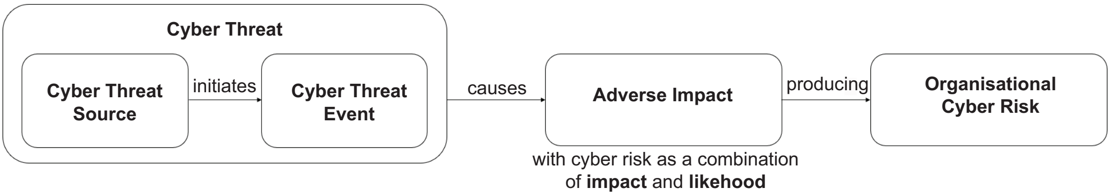

Cyber Threat
Cyber Threat Source
initiates
Cyber Threat Event
causes
Adverse Impact
producing
Organisational Cyber Risk
with cyber risk as a combination of **impact** and **likehood**

Figure 1. Cyber risk model.

serve different purposes and provide different insights. A cyber risk assessment offers a comprehensive view of an organisation's overall cyber risks, while a cyber threat assessment provides a focused analysis of the specific threats and threat actors targeting the organisation.

2.3. Terminology

The terms used in the work, that have an interpretation different from that given in NIST or ENISA glossaries, are described by the following definitions (taking into account [21, 22]):

- **organisation's network cybersecurity domain –** a set of the organisational assets and resources that are the objects of the network cybersecurity policy of the organisation;
- **network traffic –** data (encapsulated in network packets) moving between individual hosts or nodes within the network;
- **network traffic monitoring and analysis tool –** a software, hardware, or software-hardware solution whose functionality allows the usage of signature or anomaly analysis methods to detect network cyber threat events in network traffic;
- **log management tool –** a software, hardware, or software-hardware solution whose functionality allows the transmission, storage, analysis, and deletion of logs obtained from the network traffic monitoring and analysis tool (-s);
- **network cyber threat event –** an information security event detected by the network traffic monitoring and analysis tools, that means the detection of an indicator of attack or an indicator of compromise in network traffic (that is, an attempt or the fact of the network cyber threat realisation), classified according to the taxonomy of network cyber threats and characterised by criticality and the likelihood of successful realisation;
- **indicator of attack** (IoA) **–** a proactive indicator that determines the procedure, technique, tactic (TTP), according to which a network cyber threat can be successfully realised;
- **indicator of compromise** (IoC) **–** a reactive indicator that identifies a network-level artifact (classified according to the list of types of network-level artifacts), that indicates the fact of the successful network cyber threat realisation;
- **network cyber threat –** a threat that is identified through the characteristics of a network cyber threat source and a network cyber threat event (or a set of such events), the successful implementation of which involves the occurrence of undesirable consequences (harmful impact).

2.4. Conceptual Model of the Organisation's Network Cybersecurity Domain

Figure 2 represents a conceptual model of the organisation's network cybersecurity domain, considering the external and internal cyber threat surfaces. Important relationships between the entities reflected in such a high-level concept are:

- conducting cyber attacks as a way of external and internal cyber threat realisation by cyber threat sources (in the context of this work cyber threats initiated by adversaries are considered);
- transferring of network cyber threat events to the log management tool, where they are analysed for the purpose of classification and realisation of additional calculation operations (in particular, calculation of the Network Cyber Threat Score).

2.5. Organisation's Network Cyber Threat Assessment Process

There are numerous risk assessment methods available [17, 18, 23–27] and depending on the specific one employed, a risk assessment may have a number of steps or phases, and each of these phases may have slightly different names. The assessment of network cyber threats that is considered in the article is not a full-fledged measure of the cyber risk because the methodology was developed considering the common circumstances of the deficiency of the risk context data. Since the network cyber threat events detected by network traffic monitoring and analysis tools are the only source of information considered for the assessment, and due to the lack of metrics that could define important cyber risk factors, cyber threat assessment (rather than cyber risk assessment) is reviewed in this work. Guided by the approach to risk assessment defined in [17, 19, 23, 25], the stages of the network cyber threat assessment process for this methodology can be defined (see Figure 3), namely:

- preparation for the assessment;
- conducting the assessment;
- interpreting and communicating assessment results;
- maintaining the assessment.

The aim of the stage of **preparation for the assessment** is to identify the context of the network cyber threat assessment, which includes:

- identification of the purpose of the assessment;
- identification of the assessment scope;

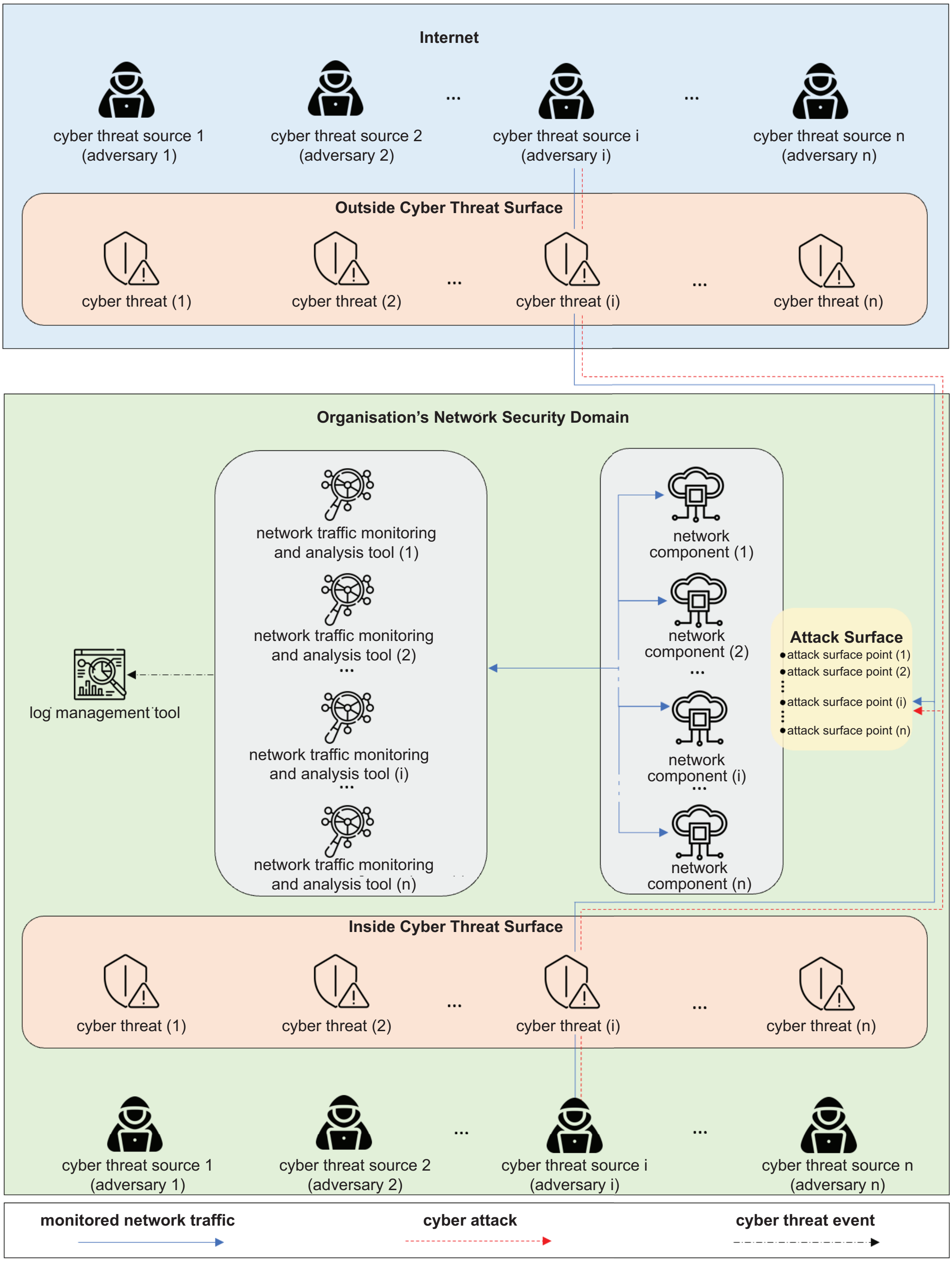

Internet
cyber threat source 1 (adversary 1)
cyber threat source 2 (adversary 2)
...
cyber threat source i (adversary i)
...
cyber threat source n (adversary n)
Outside Cyber Threat Surface
cyber threat (1)
cyber threat (2)
...
cyber threat (i)
...
cyber threat (n)
Organisation's Network Security Domain
network traffic monitoring and analysis tool (1)
network traffic monitoring and analysis tool (2)
...
network traffic monitoring and analysis tool (i)
...
network traffic monitoring and analysis tool (n)
network component (1)
network component (2)
...
network component (i)
...
network component (n)
log management tool
Attack Surface
attack surface point (1)
attack surface point (2)
attack surface point (i)
attack surface point (n)
Inside Cyber Threat Surface
cyber threat (1)
cyber threat (2)
...
cyber threat (i)
...
cyber threat (n)
cyber threat source 1 (adversary 1)
cyber threat source 2 (adversary 2)
...
cyber threat source i (adversary i)
...
cyber threat source n (adversary n)
monitored network traffic
cyber attack
cyber threat event

Figure 2. Conceptual model of the organisation`s network cybersecurity domain.

- identification of assumptions and constraints associated with the assessment;
- identification of information sources that are used as input data for conducting the assessment.

The aim of the stage of **conducting the assessment** is the calculation of the Network Cyber Threat Score, which includes:

- identification of the approach for classifying network cyber threats;
- identification of the network cyber threat characteristics, that are considered during the assessment;
- calculation of the Network Cyber Threat Score.

The aim of the stage of **interpreting and communicating assessment results** is a correct interpretation and understanding of the calculated Network Cyber Threat Score as well as a discussion of the obtained results in order to make effective managerial decisions, which includes:

- sharing the assessment results (e.g., executive briefings, assessment reports, dashboards);
- communicating assessment results in order to potentially make managerial decisions based on them.

The aim of the stage of **maintaining the assessment** is to track the trend of changes, to support making managerial decisions based on assessment results, and to incorporate any changes to the network cyber threat assessment approach if it needs to be actualised and updated, which includes:

- regular conduction of the organisation's network cyber threat assessment;
- regular review of the assessment approach.

3. Methods

3.1. Defining Common Network Cyber Threat Attributes

The purpose of the organisation's network cyber threat assessment is the calculation of a quantitative indicator that reflects the level of organisation's network cyber threats and can be used to compare the level of network cyber threats in different periods of time in order to monitor the trend of changes, as well as to support the managerial decision-making process (that means the implementation of such an indicator that would

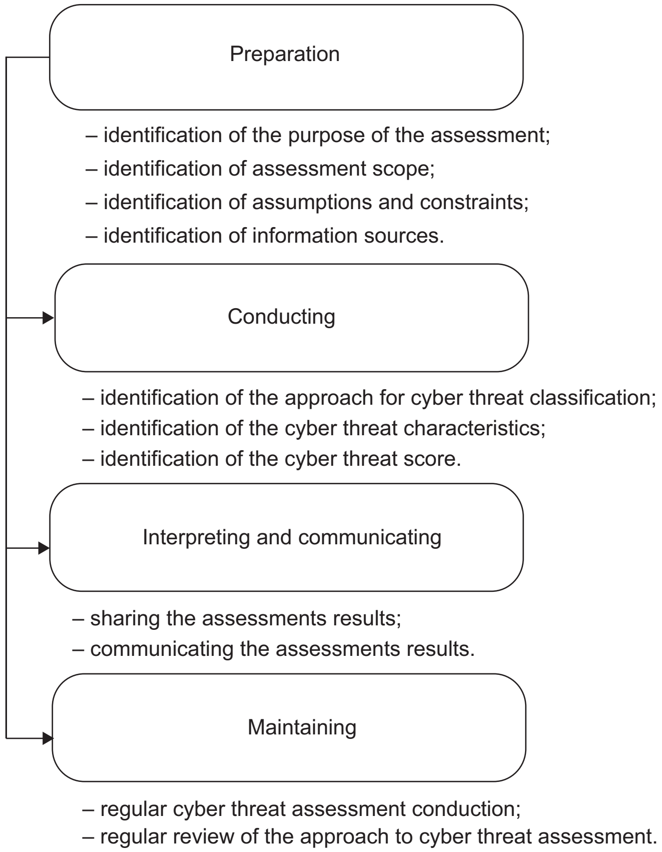

Preparation
– identification of the purpose of the assessment;
– identification of assessment scope;
– identification of assumptions and constraints;
– identification of information sources.
Conducting
– identification of the approach for cyber threat classification;
– identification of the cyber threat characteristics;
– identification of the cyber threat score.
Interpreting and communicating
– sharing the assessments results;
– communicating the assessments results.
Maintaining
– regular cyber threat assessment conduction;
– regular review of the approach to cyber threat assessment.

Figure 3. Stages of the network cyber threat assessment process.

be representative both for displaying the level of network cyber threats of a particular organisation and for comparing these levels between several organisations). Network cyber threat events, that are detected by network traffic monitoring and analysis tools, are the only **source of information considered for this assessment** in terms of the work.

Network cyber threat events can be discovered through the implementation of signature and (or) anomaly analysis methods when writing rules for detecting indicators of attacks or indicators of compromise in network traffic, that are applied to a network traffic monitoring and analysis tool. Since the quality of the written rules, according to which the network cyber threat events are detected, directly affects the quality of the subsequent events classification, **it is important to maintain and support the detection engineering**

process, which means developing, updating, validating, and testing the rules.

Network cyber threat events are the manifestations of cyber threats in a network environment that need to be detected, categorised, and mitigated [28, 29]. Network cyber threat attributes refer to specific characteristics or properties associated with network cyber threats that help in identifying, analysing, and understanding the nature and behaviour of the threats. As mentioned earlier, considering a greater number of relevant attributes contributes to increasing the objectivity and accuracy of the network cyber threat assessment process. Since the network cyber threat events detected by network traffic monitoring and analysis tools are the only source of information considered for the assessment in this work, it is essential to consider the key network cyber threat attributes to classify such events. Figure 4 represents the common network cyber threat attributes that are described in Table 1.

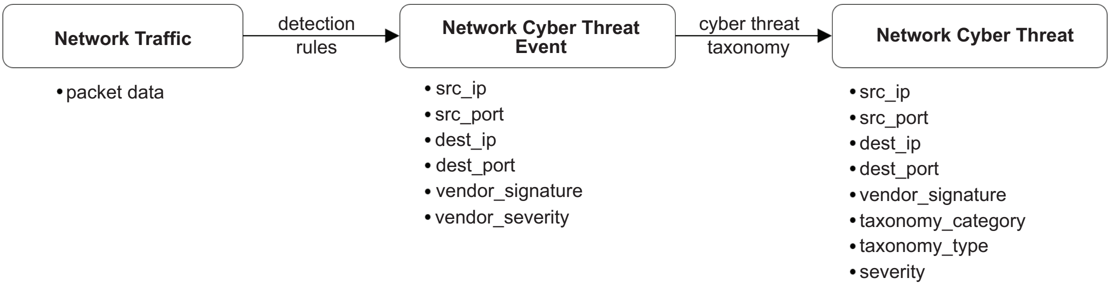


Figure 4. Network cyber threat attributes.

Table 1. Network cyber threat attributes.

Attribute name	Attribute description
src_ip	Source IP address of the network cyber threat event.
src_port	Source port of the network cyber threat event.
dest_ip	Destination IP address of the network cyber threat event.
dest_port	Destination port of the network cyber threat event.
vendor_signature	Signature of the network cyber threat event, defined by the author of the network cyber threat event detection rule.
taxonomy_category	Category of the network cyber threat event, defined after classification by the taxonomy.
taxonomy_type	Type of the network cyber threat event, defined after classification by the taxonomy.
severity	Severity of the network cyber threat event (can be defined either according to vendor_severity attribute (severity 'by default' that is defined by the author of the network cyber threat event detection rule) or reclassified using the individual approach).

3.2 Developing the Taxonomy of Network Cyber Threats

Currently, there are different ways in which to classify threats [30, 31] and it is worth noting that the categorisation is not always clear-cut. When dealing with the topic of threat event classification **it is not possible to determine which the best or correct classification is** because organisations defining a taxonomy are usually driven by different needs and have different expectations. It is determined in NIST [17] that the **network cyber threat event classification can be carried out at one of the levels of detail necessary for describing such an event**, depending on the existing assessment requirements. Description of the network cyber threat events can be general (e.g., phishing, distributed denial-of-service attack, etc.), more specific (identification of involved tactics, techniques, and procedures), or highly specific (relating to specific information systems, technologies, organisations, roles, or locations).

It would seem that creating a unified Network Cyber Threats Taxonomy is crucial for improving the detection, classification, and response to network cyber threats. It fosters standardisation, enhances collaboration, supports automation, and, ultimately, leads to a more cohesive and effective cybersecurity posture across organisations and even industries. However, while a uniform Network Cyberthreats Taxonomy offers numerous benefits, there are many scenarios where developing or modifying different taxonomies can be advantageous. The tailored approach ensures that the diverse and evolving nature of cyber threats is adequately addressed in various contexts.

Considering [32–35], the **Network Cyber Threat Taxonomy was developed** (see Table 2). It allows to correlate the detected network cyber threat events with the corresponding cyber threat types and categories (i.e., to classify the detected network cyber threat events). The aim of the proposed Network Cyber Threat Taxonomy is not to enable the community to reach a consensus on a reference taxonomy, but rather to propose one of the possible implementation options and additionally emphasise the significance and criticality of a properly adopted taxonomy in the task of threat classification.

3.3. Calculating, Normalisation, and Interpretation of the Network Cyber Threat Score

During the selection of the method for calculating the Network Cyber Threat Score, a comparative analysis was conducted between the qualitative and quantitative approaches [36–39].

Table 2. Network cyber threat taxonomy.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Malware infection	Detection of network artifacts or network behaviour that indicate a malware infection. Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.	**stealer**	Detection of network activity that indicates known stealer infection.
		spyware	Detection of network activity that indicates known spyware infection.
		RAT	Detection of network activity that indicates known RAT infection.
		trojan	Detection of network activity that indicates known trojan infection.
		worm	Detection of network activity that indicates known worm infection.
		browser malware	Detection of network activity that indicates known browser malware infection.
		cryptomining malware	Detection of network activity that indicates known cryptomining malware infection.
		post-exploitation tool	Detection of network activity that indicates known post-exploitation tool infection.
		loader (dropper)	Detection of network activity that indicates known loader infection.
		as-a-service malware tool	Detection of network activity that indicates known as-a-service malware tool infection. *Example: detection of malware-as-a-service tool, phishing-as-a-service tool, ransomware-as-a-service tool infection.*
		proxy malware	Detection of network activity that indicates known proxy malware infection.
		rootkit	Detection of network activity that indicates known rootkit infection.
		ransomware	Detection of network activity that indicates known ransomware infection.
		misused legitimate tool	Detection of network activity that indicates s known legitimate tool that is often misused.
		malware (unclassified)	Detection of network activity that cannot be directly attributed to known malware type but still indicates malware infection. *Example: detection of anomalous network behaviour, related to malware infection.*

(*continues*)

Table 2. Continued.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Threat Actors activity	Detection of network artifacts, related to targeted activity. These are artifacts of sophisticated, long-term cyber attack campaigns (usually involve a series of coordinated and targeted attacks) that are typically carried out by a well-resourced and highly skilled threat actors and focus on specific organisations/entities or whole geographic regions.Categories of cybersecurity Threat Actors, that are considered: • State-sponsored actors • Cybercrime actors • Hacker-for-hire actors • Hacktivists	**malicious network connection**	Detection of network connections to the malicious infrastructure that can be attributed to the known Threat Actor.
Suspicious network activity	Detection of network artifacts or anomalous behaviour that indicates suspicious network activity. Suspicious network activity means a potentially unwanted activity that cannot be clearly identified as a malicious one but can cause undesirable impact. When observed in conjunction with other artifacts or behaviour, they can help identify and investigate true positive security incidents or intrusions.	**anomalous network traffic behaviour**	Detection of network anomalies (spikes, unexpected or unusual communication patterns and so on). *Example: detection of anomalous network behaviour, that indicates data hoarding or network misconfiguration.*
		accessing configuration file	Detection of network activity that indicates access to a configuration file.
		suspicious network connection	Detection of network activity that indicates suspicious (potentially malicious) connections. *Example: detection of connections to a free web hosting service/a non-existent page, the usage of anonymous services, detection of suspicious user-agent string or content type.*
		scanning	Detection of network activity that indicates scanning. *Example: detection of web scanning, port/ping scanning.*

(*continues*)

Table 2. Continued.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Malicious network activity	Detection of network artifacts or behaviour, that indicates malicious network activity. Malicious network activity means unwanted activity that causes undesirable impact (disruption or exploiting systems, data, or network resources).	**malware distribution**	Detection of network activity that indicates malware distribution.
		disrupting availability	Detection of network activity that indicates availability disruption. Availability disruption means making relevant data, services, or other resources unavailable for access by users of a system or service. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. *Example: detection of dos, ddos attempts.*
		unauthorised login	Detection of network activity that indicates unauthorised login attempts (includes one try or multiple tries). *Example: detection of default credentials login, brute force attempts.*
		file download/ upload	Detection of network activity that indicates file upload or download attempt.
		threats against data	Detection of network activity that indicates threats against data. *Example: detection of data leak, data exfiltration (breach) attempts.*
		directory/path traversal	Detection of network activity that indicates directory/path traversal attempt.
		injection	Detection of network activity that indicates injection attempt. *Example: detection of command, code, sql, xss, php injection attempts.*
		webshell	Detection of network activity that indicates webshell upload or download attempt.
		remote code execution	Detection of network activity that indicates remote code execution attempt.
		malicious network connection	Detection of network activity blacklisted by the reputation.

The qualitative approach relies on non-numerical descriptive data and subjective analysis [40], and involves expert opinions, insights, and experiences to evaluate cyber threats. The main advantage of adopting the qualitative approach is that it can be applied in situations where quantitative data are limited or unavailable. Conversely, the quantitative approach relies on measurable data and statistical techniques, utilises metrics, scores, and other numerical values derived from data analysis to assess threats. The main advantage of adopting the quantitative approach lies in reducing biases [41] by relying on numerical data and statistical methods.

It is of the belief that there is no way to completely eliminate subjectivity in risk scoring [42] even with a fully quantitative methodology. In practice, the combination of both approaches is often used for a more comprehensive and balanced assessment of network cyber threats. However, in this work, the quantitative approach was preferred because it offers clear, quantitatively defined results that facilitate comparison and prioritisation.

To achieve the assessment goal, two values of the Network Cyber Threat Score (maximum and average) are proposed to be calculated, with each being more representative of specific cases.

The maximum value of the organisation's Network Cyber Threat Score ($S_{threat(max)\_normalized}$) is proposed to be used as a quantitative indicator that reflects the level of network cyber threats of a specific organisation. It takes the value of the maximum score among all the calculated normalised Network Cyber Threat Scores $S_{threat(i)\_normalized}$. In this case, $S_{threat(max)\_normalized}$ score value provides insight into the most critical network cyber threat that has been detected in the organisation's network traffic during the defined time period.

The average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$) is proposed to be used as a quantitative indicator that can be implemented to compare the network cyber threat levels of several organisations. It takes the average value among all the calculated normalised Network Cyber Threat Scores ($S_{threat(i)\_normalized}$). In this case, ($S_{threat(avg)\_normalized}$) score value provides a general understanding of the organisation's network cyber threat landscape.

The Network Cyber Threat Score $S_{threat(i)}$ is proposed to be calculated using the mixed method, considering the network cyber threat characteristics (that are defined by network cyber threat event characteristics, namely severity and likelihood of successful realisation [43, 44]):

$$S_{threat(i)} = S_{detection(i)} \times (S_{severity(i)} + S_{likelihood(i)} + S_{frequency(i)}) \qquad (1),$$

where: i = 1,2,…,n, n – the total number of network cyber threat types that are detected and taken into account during the assessment time period;

$S_{detection(i)}$ – **detection factor**, which is represented by the quantitative detection score value of the network cyber threat (see Table 3);

$S_{severity(i)}$ – **severity factor**, which is represented by the quantitative severity score value of the network cyber threat (see Table 4);

$S_{likelihood(i)}$ – **likelihood factor**, which is represented by the quantitative likelihood score value of the network cyber threat (see Table 5);

$S_{frequency(i)}$ – **frequency factor**, which is represented by the quantitative frequency score value of the network cyber threat (see Table 6).

Table 3. Categories of the Network Cyber Threat Detection Score values ($S_{detection(i)}$).

Qualitative value	Quantitative value	Category description
Detected	1	Cyber threat is considered detected if some alert (from any security monitoring or analysis hardware/software tool operating within the organisational network) that indicates the cyber network threat type presence during the assessment period exists, i.e., the **number of detections is not equal to zero**.
Not Detected	0	Cyber threat is considered not detected if any alert (from any security monitoring or analysis hardware/software tool operating within the organisational network) that indicates the cyber network threat type presence during the assessment period doesn`t exists, i.e. **the number of detections is equal to zero**.

Table 4. Categories of the Network Cyber Threat Severity Score values ($S_{severity(i)}$).

Qualitative value	Quantitative value	Category description
Low	1	Cyber threat is within the low severity level if **it has no impact at all or potentially minor impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.
Medium	2	Cyber threat is within the medium severity level if **it has a potentially moderate impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.
High	3	Cyber threat is within the high severity level if **it has a potentially severe impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.

Table 5. Categories of the Network Cyber Threat Likelihood Score values ($S_{likelihood(i)}$).

Qualitative value	Quantitative value	Category description
Low	1	Cyber threat is within the low likelihood level if it is **detected in the organisation`s inbound network traffic that gives grounds to characterise the successful implementation of its potential impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation **with a low level of confidence**.
High	2	Cyber threat is within the high likelihood level if it is **detected in the organisation`s outbound network traffic that gives grounds to characterise the successful implementation of its potential impact** on the stable, reliable and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation **with a high level of confidence**.

Table 6. Categories of the Network Cyber Threat Frequency Score values ($S_{frequency(i)}$).

Qualitative value	The method of normalisation of the absolute value of detections	Quantitative value	Category description
Low	$S_{frequency(i)} = \log_{10}(x+1)$	$0 < S_{frequency(i)} \leq 1$	The frequency of detections is low if the absolute value of detections of this network cyber threat type (x) meets the condition: $1 \leq x \leq 10$
Medium		$1 < S_{frequency(i)} < 2$	The frequency of detections is medium if the absolute value of detections of this network cyber threat type (x) meets the condition: $10 < x < 100$
High		$S_{frequency(i)} \geq 2, S_{frequency(max)} = 3$ For $S_{frequency(i)} \geq 3$: $S_{frequency(i)} = S_{frequency(max)}$	The frequency of detections is high if the absolute value of detections of this network cyber threat type (x) meets the condition: $x \geq 100$

In this formula, the multiplicative and additive approaches are combined [45, 46]. The multiplicative component $S_{detection(i)}$ represents the detection confidence. The additive component represents a balanced combined effect of the severity ($S_{severity(i)}$), likelihood ($S_{likelihood(i)}$), and frequency ($S_{frequency(i)}$) factors, where each factor is added to reflect their contribution to the overall Network Cyber Threat Score value.

Taking into account the difference in the impact of severity, likelihood, and frequency factors on the resulting score, **weighting**

coefficients $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ **were determined** [47] by the method of individual expert assessment. A subject matter expert (SME) assessment approach is often criticised because of potential biases [48] based on experiences or affiliations, which can influence the assessment results, as well as because of the need to consider and assess the level of expertise related to a specific narrow research topic. However, the competent management of these considerations helps to maximise the benefits of using the SME assessment approach [49]: credibility, reliability (despite a certain degree of subjectivity, involving experts adds authority and trustworthiness to the findings), and insight (SMEs can provide precise and credible evaluations based on their experience and a thorough understanding of nuanced complex topics).

In the scoring method, x_{ij} – is the weighting coefficient of the *i*-th factor that is defined by the *j*-th expert, $i = \overline{1,n}$, $j = \overline{1,m}$. Herewith, *n* – is the total number of the factors, that are compared, *m*- is the total number of experts (in our case, *n* = 3, *m* = 5).

Thus, a group of five SMEs was selected, whose task was to determine the weighting coefficients $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ (by the method of direct assessment expressed in points), considering the condition that the sum of these weighting factors should be 10 points.

Using the **coefficient of variation** (*V*) we can analyse the extent of variability of determined expert scores $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ and therefore check their reliability (the relative dispersion of data points in a data series around the mean). It is calculated according to the formula:

$$V = \frac{\sigma}{\overline{x}} \times 100\% \qquad (2),$$

where: *V* – coefficient of variation;

σ – mean squared deviation (MSD) of expert scores that is calculated according to (3);

$\overline{x}$ – arithmetic mean of expert scores that is calculated according to (4).

$$\sigma = \sqrt{\frac{\sum_{j=1}^{m}\left(x_{i,j} - \overline{x}\right)^2}{m-1}} \qquad (3),$$

where: σ – mean squared deviation (MSD) of expert scores;

$x_{i,j}$ – score of the *i*-th factor that is defined by the *j*-th expert;

$\bar{x}$ – arithmetic mean of expert scores;

m – the total number of experts.

$$\bar{x} = \frac{\sum x_{i,j}}{n} \qquad (4),$$

where: $\bar{x}$ – arithmetic mean of expert scores;

$x_{i,j}$ – score of the *i*-th factor that is defined by the *j*-th expert;

n – the total number of factors that are evaluated.

The calculated values of variation coefficients *V* (see Table 5) indicate low values of variation for $w_{severity}$, $w_{likelihood}$ (that means the high homogeneity of the respective data sets (low variability) and that the arithmetic mean value is a reliable characteristic for them), as well as a moderate value of variation for $w_{frequency}$ (that means moderate homogeneity of the corresponding data set and the fact that instead of the arithmetic mean value, it is more appropriate to choose the mode or median as a characteristic of the distribution centre).

Therefore, the resulting weighting coefficients for the *i*-th factors, pre-assessed according to the experts' scores (w_i), are determined by the modes (by the values that are most often found in the sets of weights ($x_{i,j}$) for the *i*-th factors, assessed by the scores of the *m* number of experts, i.e., have the highest frequency $f(w_{i,j})$.

Table 7. The defined values of the weighting coefficients for the Network Cyber Threat Score factors and the values of variation coefficients.

Weight score of the *i*-th factor	**Score of the *j*-th expert**					$\bar{x}$	**σ**	***V***	**Frequency of the weight score ($f(w_{ij})$)**	**Resulting weight score (w_i)**
	***j* = 1** w_{i1}	***j* = 2** w_{i2}	***j* = 3** w_{i3}	***j* = 4** w_{i4}	***j* = 5** w_{i5}					
$i = 1, w_{1j}\,(w_{severity})$	$x_{1,1}$ 5	$x_{1,2}$ 6	$x_{1,3}$ 6	$x_{1,4}$ 5	$x_{1,5}$ 6	5.6	0.55	9,82%	$f(w_{1j} = 5) = 2$ $f(w_{1j} = 6) = 3$	6
$i = 2, w_{2j}\,(w_{likelihood})$	$x_{2,1}$ 4	$x_{2,2}$ 3	$x_{2,3}$ 3	$x_{2,4}$ 3	$x_{2,5}$ 3	3.2	0.45	14,06%	$f(w_{2j} = 3) = 4$ $f(w_{2j} = 4) = 1$	3
$i = 3, w_{3j}\,(w_{frequency})$	$x_{3,1}$ 1	$x_{3,2}$ 1	$x_{3,3}$ 1	$x_{3,4}$ 2	$x_{3,5}$ 1	1.2	0.45	37,5%	$f(w_{3j} = 1) = 4$ $f(w_{3j} = 1) = 1$	1

Taking into account the determined weights from Table 7 equation (1) takes the form:

$$S_{threat(i)} = S_{detection(i)} \times ((w_{severity} \times S_{severity(i)}) + (w_{likelihood} \times S_{likelihood(i)}) + (w_{frequency} \times S_{frequency(i)})) \quad (5)$$

For convenient interpretation of the Network Cyber Threat Score value, **normalisation** (converting the calculated values to the required scale) is applied by using the linear scaling formula [50]:

$$S_{threat(i)\_normalized} = \left(\frac{S_{threat(i)} - S_{threat(min)}}{S_{threat(max)} - S_{threat(min)}}\right) \times \left(S_{threat(max)\_normalized} - S_{threat(min)\_normalized}\right) + S_{threat(min)\_normalized} \quad (6),$$

where: $S_{threat(min)} = 1 \times ((6 \times 1) + (3 \times 1) + (1 \times 0.3)) = 9.3$ (the minimal value of not normalised range);

$S_{threat(max)} = 1 \times ((6 \times 3) + (3 \times 2) + (1 \times 3)) = 27$ (the maximum value of not normalised range);

$S_{threat(min)\_normalized} = 1$ (the minimal value of normalised range);

$S_{threat(max)\_normalized} = 100$ (the maximum value of normalised range).

Considering that $S_{threat(i)\_normalized}$ values for not detected network cyber threats correspond to the same $S_{threat(i)}$ values and are equal to zero, we get normalised (see Table 8) interpretable (see Table 9) ranges of the Network Cyber Threat Score [0,100].

The boundary values in Tables 8 and 9 are preliminary and almost evenly distributed, but in practice, they should be chosen in accordance with the determined level of risk tolerability [51–55] and revised regularly as the risk landscape evolves [56]. Setting boundaries helps in categorising and prioritising risks accurately [57, 58]. That's why setting the tolerability level should be tailored to the unique context [59] and be established periodically by decision makers at a strategic level in accordance with the external risk environment of the organisation and relevant justification, that in some cases becomes a contractual objective.

The average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$), as a normalised average score of all detected

Table 8. Normalised ranges of the Network Cyber Threat Score values.

Detection categories	Severity categories	Likelihood categories	Frequency categories	Resulting category (not normalised values)	Resulting category (normalised values)
Not Detected (0)	*	*	*	Undefined (0)	
Detected (1)	Low (6)	Low (3)	Low (1)	Informational (9.3, 10]	Informational (1, 4.9]
			Medium (2)	Informational (10, 11)	Informational (4.9, 10.5)
			High (3)	Informational [11, 12]	Informational [10.5, 16.1]
	Low (6)	High (6)	Low (1)	Low (12, 13]	Low (16.1, 21.7]
			Medium (2)	Low (13, 14)	Low (21.7, 27.3)
			High (3)	Low [14, 15]	Low [27.3, 32.9]
	Medium (12)	Low (3)	Low (1)	Medium (15, 16]	Medium (32.9, 38.5]
			Medium (2)	Medium (16, 17)	Medium (38.5, 44.1)
			High (3)	Medium [17, 18]	Medium [44.1, 49.7]
	Medium (12)	High (6)	Low (1)	Medium (18, 19]	Medium (49.7, 55.3]
			Medium (2)	Medium (19, 20)	Medium (55.3, 60.8)
			High (3)	Medium [20, 21]	Medium [60.8, 66.4]
	High (18)	Low (3)	Low (1)	High (21, 22]	High (66.4, 72]
			Medium (2)	High (22, 23)	High (72, 77.6)
			High (3)	High [23, 24]	High [77.6, 83.2]
	High (18)	High (6)	Low (1)	Critical (24, 25]	Critical (83.2, 88.8]
			Medium (2)	Critical (25, 26)	Critical (88.8, 94.4)
			High (3)	Critical [26, 27]	Critical [94.4, 100]

Table 9. Categories of Network Cyber Threat Score values (interpretation).

Qualitative value	Quantitative value	Description
Undefined level	$S_{threat(i)\_normalized} = 0$	If the calculated **Network Cyber Threat Score value** is **within the undefined level**, this **indicates** that **there were no network cyber threat type detections** in the organisation`s inbound or outbound network traffic during the evaluated time period.
Informational level	$1 < S_{threat(i)\_normalized} \leq 16.1$	If the calculated **Network Cyber Threat Score value** is **within the informational level**, this **indicates** that **a low criticality network cyber threat type with a low likelihood level of successful realisation** was detected in the organisation`s inbound network traffic during the evaluated time period. The information level category doesn`t require the organisation's response to take measures related to the detected cyber threat type, as it potentially doesn`t cause a significant impact on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Low level	$16.1 < S_{threat(i)\_normalized} \leq 32.9$	If the calculated **Network Cyber Threat Score value** is **within the low level**, this **indicates** that **a low criticality network cyber threat type with a high likelihood level of successful realisation** was detected in the organisation`s outbound network traffic during the evaluated time period. The low level category doesn`t require the organisation's response to take measures related to the detected cyber threat type, as it potentially doesn`t cause a significant impact on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Medium level	$32.9 < S_{threat(i)\_normalized} \leq 66.4$	If the calculated **Network Cyber Threat Score value** is **within the medium level**, this **indicates** that **a medium criticality network cyber threat type** was detected in the organisation`s inbound or outbound network traffic during the evaluated time period. The medium-level category requires the organisation's response to take measures related to the detected cyber threat type, as it can potentially cause a significant impact on the stable, reliable and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.

(*continues*)

Table 9. Continued.

Qualitative value	Quantitative value	Description
High level	$66.4 < S_{threat(i)\_normalized} \leq 83.2$	If the calculated **Network Cyber Threat Score value** is **within the high level**, this **indicates** that **a high criticality network cyber threat type with a low likelihood level of successful realisation** was detected in the organisation`s inbound network traffic during the evaluated time period. The high-level category requires the immediate organisation’s response to take measures related to the detected cyber threat type (localising and eliminating the potential consequences), as it can potentially cause a significant impact on the stable, reliable, and regular functioning of the organisation’s informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Critical level	$83.2 < S_{threat(i)\_normalized} \leq 100$	If the calculated **Network Cyber Threat Score value** is **within the critical level**, this **indicates** that **a high criticality network cyber threat type with a high likelihood level of successful realisation** was detected in the organisation`s outbound network traffic during the evaluated time period. The critical level category requires the immediate organisation’s response to take measures related to the detected cyber threat type (localising and eliminating the consequences), as it can have a significant impact on the stable, reliable and regular functioning of the organisation’s informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the cyber risk.

network cyber threats is proposed to be calculated using the formula of the arithmetic mean, since the individual values of the averaged feature (normalised Network Cyber Threat Scores) and their number in the aggregate are known:

$$S_{threat(avg)\_normalized} = \frac{1}{k} \times \sum_{i=1}^{k} S_{threat(i)\_normalized} \qquad (7),$$

where: $i = 1, 2, \ldots, k$, k – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment and for which the absolute number of detected cyber threat events is a non-zero value, meaning $x \neq 0$; $\sum_{i=1}^{k} S_{threat(i)\_normalized}$ – the sum of the detected normalised Network Cyber Threat Scores.

The arithmetic mean is commonly used in various risk assessment and scoring methodologies as it provides an intuitive and easily interpretable measure of the central tendency. Since the individual Network Cyber Threat Scores are normalised, they are on a comparable scale, making the arithmetic mean an appropriate measure. By averaging all normalised Network Cyber Threat Scores, the arithmetic mean accounts for the cumulative impact of all the detected threats and appears to be a consistent metric, meaning that changes in individual normalised Network Cyber Threat Score values will proportionately affect the overall average and contribute equally, avoiding bias from extreme values. Therefore, it can serve as a baseline metric for comparing changes in the organisation's network cyber threat landscape over time as well as for comparing network security postures of different organisations.

Table 10 represents categories, according to which the calculated average value of the organisation's Network Cyber Threat Score is proposed to be interpreted.

4. Results

According to the methodology, presented in the work, a scheme of the algorithm was developed (see Figure 5) for the automated calculation of the Network Cyber Threat Score, where: *j* – the overall number of detected network cyber threat events during the assessment period; *n* – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment (according to the taxonomy, proposed to use in this work, $n = 30$); *k* – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment and for which the absolute number

Table 10. Categories of the average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$).

Qualitative value	Quantitative value	Description
Undefined level	$S_{threat(avg)\_normalized} = 0$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **undefined**.
Low level	$1 < S_{threat(avg)\_normalized} \leq 32.9$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the low-level** range.
Medium level	$32.9 < S_{threat(avg)\_normalized} \leq 66.4$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the medium-level** range.
High level	$66.4 < S_{threat(avg)\_normalized} \leq 100$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the high-level** range.

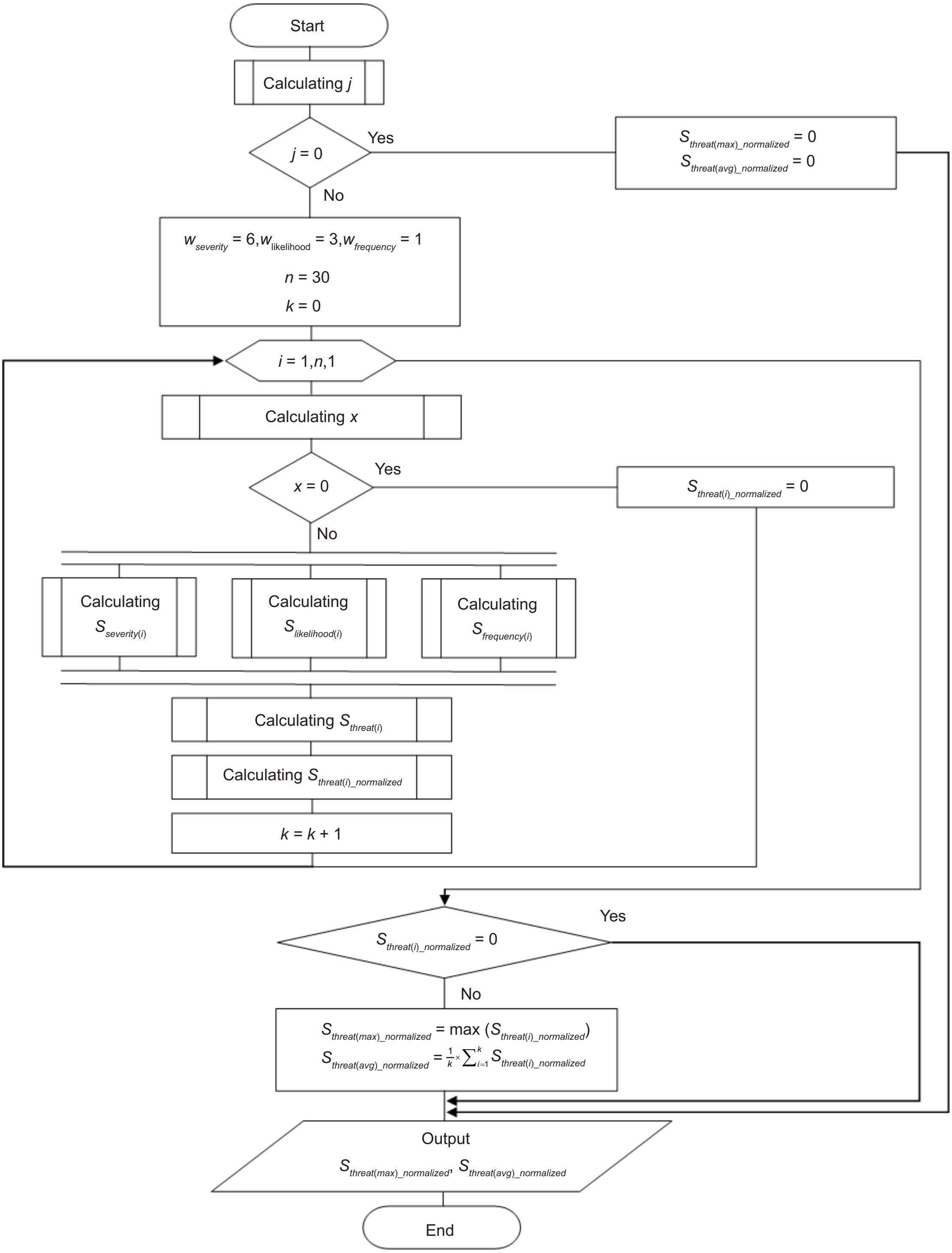

Start
Calculating j
$j = 0$
Yes
No
$S_{threat(max)\_normalized} = 0$
$S_{threat(avg)\_normalized} = 0$
$w_{severity} = 6, w_{likelihood} = 3, w_{frequency} = 1$
$n = 30$
$k = 0$
$i = 1,n,1$
Calculating x
$x = 0$
Yes
No
$S_{threat(i)\_normalized} = 0$
Calculating $S_{severity(i)}$
Calculating $S_{likelihood(i)}$
Calculating $S_{frequency(i)}$
Calculating $S_{threat(i)}$
Calculating $S_{threat(i)\_normalized}$
$k = k + 1$
$S_{threat(i)\_normalized} = 0$
Yes
No
$S_{threat(max)\_normalized} = \max(S_{threat(i)\_normalized})$
$S_{threat(avg)\_normalized} = \frac{1}{k} \times \sum_{i=1}^{k} S_{threat(i)\_normalized}$
Output
$S_{threat(max)\_normalized}, S_{threat(avg)\_normalized}$
End

Figure 5. A scheme of the algorithm.

of detected cyber threat events is a non-zero value, meaning $x \neq 0$; k – the absolute number of detected network cyber threat events, that are classified by network cyber threat types according to the taxonomy, proposed to use in this work.

The algorithm's scheme formalises the inputs, processes, and outputs needed to grasp and implement the steps involved in calculating the maximum ($S_{threat(max)\_normalized}$) and average ($S_{threat(avg)\_normalized}$) values of the Network Cyber Threat Score. By following these steps, the algorithm can be applied and automated for the purpose of conducting the organisation's network cyber threat assessment process more effectively, delivering real-time insights into the network's security posture and allowing for timely responses.

Taking into consideration the conceptual model of the organisation's network cybersecurity domain (presented in Figure 2), the algorithm scheme (presented in Figure 5) was validated in practice by its implementation in the log management tool of a specific organisation, allowing for the automated calculation of the Network Cyber Threat Score.

The dashboard was also developed for the log management tool, used within the organisation (see Figure 6). It visualises the results of the custom correlation searches that classify network cyber threat events with regard to the categories and types outlined in the Network Cyber Threat Taxonomy and contains the detailed results of the Network Cyber Threat Score calculation with all the related metrics. Grouping panels together and arranging them in a logical and visually appealing layout makes the dashboard easy to interpret. Therefore, the presented visualisation example can be used as one of the options for displaying the results of the algorithm implementation and for monitoring the Network Cyber Threat Score value (continuously or at scheduled intervals) to check for exceeding certain thresholds. It can be applied for sharing information developed in the execution of the cyber threat assessment during the stage of communicating and sharing assessment information. In particular, the dashboard panel contains:

1. the results of calculating the maximum and average values of the Network Cyber Threat Score (single value visualisation);
2. distribution of the number of detected cyber threat events by cyber threat categories (pie chart visualisation);
3. timechart of the number of detected cyber threat events by cyber threat categories (single value visualisation with trend indicator);

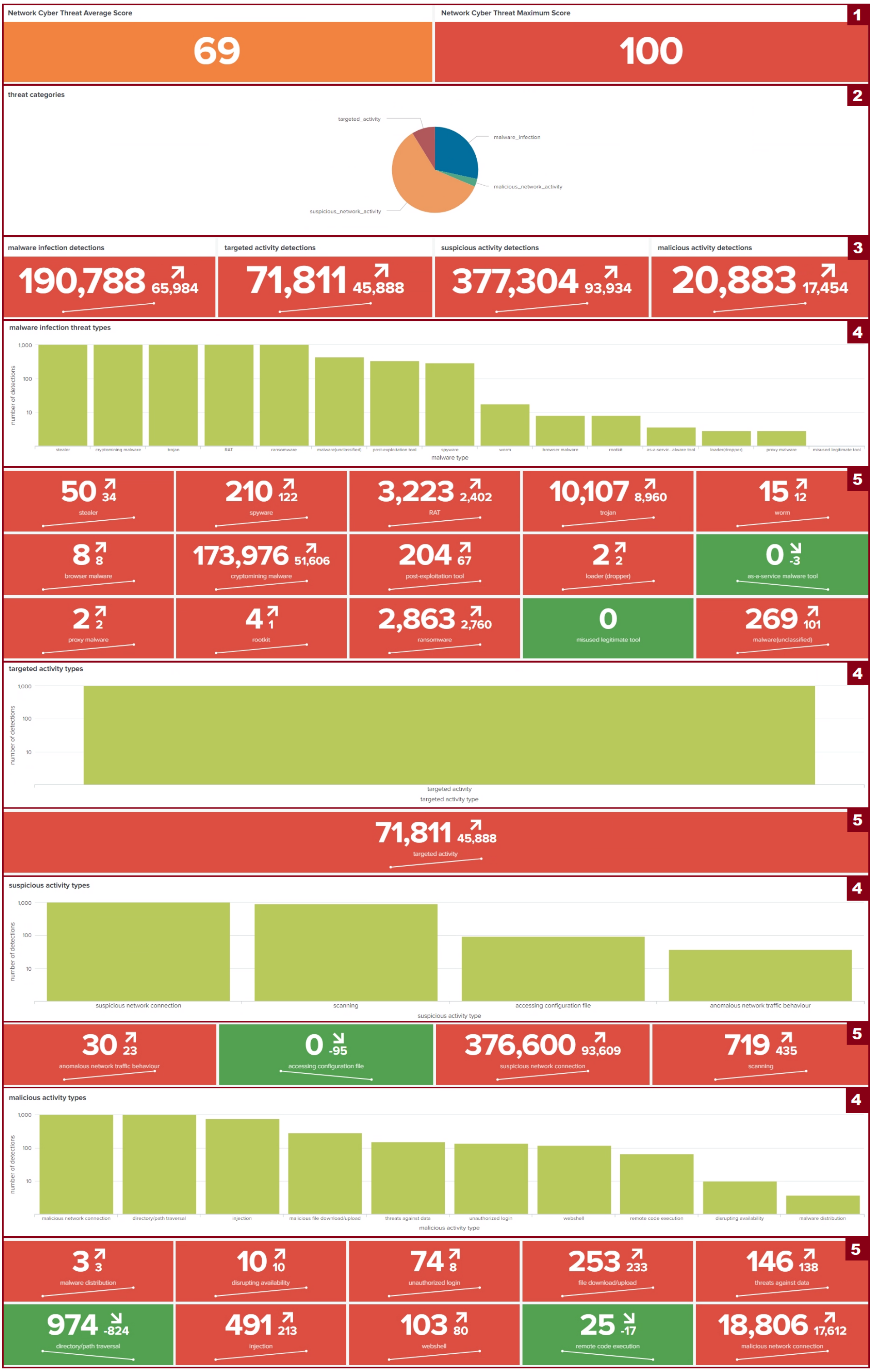


Figure 6. A dashboard panel.

4. distribution of the number of detected cyber threat events by cyber threat types (histogram visualisation);
5. timechart of the number of detected cyber threat events by cyber threat types (single value visualisation with trend indicator).

5. Discussion

A uniform approach to calculating the organisation's Network Cyber Threat Score that involves a fixed set of factors, an assessment scale for each factor, and an algorithm for combining these factors cannot simultaneously satisfy the needs of different organisations. Therefore, the creation of an adapted methodology is a necessary step in order to take into account additional factors, determine the required level of their decomposition and select a convenient combining algorithm for conducting such an assessment.

The automated calculation of the maximum and average values of the Network Cyber Threat Score according to the methodology presented in the work allows determining the quantitative indicators that **partially reflect the overall level of the organisation's cyber risk** (because network traffic analysis can detect only a certain range of cyber threats and cannot replace a complex approach to conducting a cyber risk assessment). It can be implemented **for comparing the level of network cyber threats during different time periods** to monitor the trend of changes, as well as **for supporting the process of making managerial decisions regarding the organisation's cybersecurity strategy** (namely, planning new and improving existing preventive protection measures). The methodology of calculating the Network Cyber Threat Score is also flexible enough to be adopted by various organisations by adjusting it to their own Network Cyber Threat Taxonomy. According to their requirements, the scoring of some cyber threat types and categories (the Network Cyber Threat Severity Score values) can be adjusted to produce the most appropriate results.

In terms of limitations, it is important to take into consideration the factors that directly affect the objectivity of the calculated scores:

- the technical component, namely the functional capabilities (methods of analysis) of the available network traffic monitoring and analysis tools that are in use;
- the quality of the detection rules applied directly to the existing network traffic monitoring and analysis tools for detecting network events, classified as cyber threats.

The greater the number of methods or their combinations used by the available network traffic monitoring and analysis tools, as well as the better the quality of implemented detection rules, the greater the number of network events, classified as cyber threats, can be detected and the more accurate these detections will be (in terms of increasing the number of True Positive alerts).

Currently, some simplifications of the risk-based approach are being applied to conduct the network cyber threat assessment process within the discussed methodology. Future research directions include decomposing the current procedure to define categories of Network Cyber Threat Severity and Likelihood Scores, as well as considering the other possible characteristics of network cyber threats to quantify and account for them in the calculation of the Network Cyber Threat Score.

Acknowledgements

We are thankful to our colleagues who offered their perspectives during informal discussions, which have enriched our understanding and interpretation of the researched data. First and foremost, our sincere thanks go to Mike Harbison (Engineer at Palo Alto Networks UNIT 42 team), whose guidance and insightful feedback were instrumental in shaping the research. We are also grateful to Ganna Korniychenko (Senior Threat Intelligence Analyst at KPMG UK) whose expertise and constructive suggestions significantly enhanced the quality of our work. This work is a result of the collaborative spirit and collective effort of all involved, and we are profoundly grateful for each contribution.

References

[1] Y. Yuan, W. Xu, "Network security situation based on big data environment." 6th International Workshop on Advanced Algorithms and Control Engineering (IWAACE 2022), 2022, doi: 10.1117/12.2653255.

[2] J. Zhang, H. Feng, B. Liu, D. Zhao, "Survey of technology in network security situation awareness," *Sensors*, vol. 23, no. 5, p. 2608, 2023, doi: 10.3390/s23052608.

[3] B. Zhou, B. Sun, T. Zang, Y. Cai, J. Wu, H. Luo, "Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities," *Entropy*, vol. 25, no. 1, p. 47, 2023, doi: 10.3390/e25010047.

[4] M.S. Kacar, K. Oztoprak, "Network security scoring." IEEE 11th International Conference on Semantic Computing (ICSC), 2017. [Online]. Available: https://

www.researchgate.net/publication/315872054_Network_Security_Scoring. [Accessed: Jun. 15, 2023].

[5] T. Ali, M. Al-Khalidi, Rabab Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," *The Journal of Computer Information Systems*, pp. 1–28, 2024, doi: 10.1080/08874417.2024.2329985.

[6] Imperva. (2023). *Cyber Threat Index. Cyber Security Statistics & Trends*. [Online]. Available: https://www.imperva.com/cyber-threat-index/. [Accessed: Aug. 22, 2023].

[7] NordVPN. (2020). *Cyber Risk Index.* [Online]. Available: https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf. [Accessed: Aug. 29, 2023].

[8] M. Khudyntsev, O. Lebid, M. Bychenok, A. Zhylin, A. Davydiuk, "Network monitoring index in the information security management system of critical information infrastructure objects," in *Information and Communication Technologies and Sustainable Development*, S. Dovgyi, O. Trofymchuk, V. Ustimenko, L. Globa, Eds., Lecture Notes in Networks and Systems, Springer, Cham, 2022, pp. 270–290.

[9] V. Kravets, "Comparative analysis of the cybersecurity indices and their applications," *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, pp. 97-102, 2019, doi: 10.20535/tacs.2664-29132019.1.169090.

[10] R. Xi, X. Yun, Z. Hao, Y. Zhang, "Quantitative threat situation assessment based on alert verification," *Security and Communication Networks*, vol. 9, no. 13, pp. 2135–2142, 2016, doi: 10.1002/sec.1473.

[11] H. Hu, H. Zhang, Y. Liu, Y. Wang, "Quantitative method for network security situation based on attack prediction," *Security and Communication Networks*, vol. 2017, no. 1, pp. 1–19, 2017, doi: 10.1155/2017/3407642.

[12] I. Kozubtsov, O. Chernonoh, L. Kozubtsova, M. Artemchuk, I. Neshcheret, "Selection of individual indicators for assessing the ability of the information security and cybersecurity system to function in special communication information and communication systems," *Cybersecurity: Education, Science, Technique*, vol. 16, no. 4, pp. 19–27, 2022, doi: 10.28925/2663-4023.2022.16.1927.

[13] I. Pyskun, Y. Tkach, V. Khoroshko, Y. Khokhlachova, A.R.A. Ayasrah, A.F. Al-Dalvash, "Quantitative assessment and determination of the level of cyber security of state information systems," *Ukrainian Scientific Journal of Information Security*, vol. 26, no. 3, pp. 131–138, 2020, doi: 10.18372/2225-5036.26.14974.

[14] L. Kozubtsova, Y. Khlaponin, I. Kozubtsov, "Methods of evaluation of efficiency of implementation of cyber security measures of critical information infrastructure bodies of the body. Modern information technologies in the sphere of security and defence," *Modern Information Technologies in the Field of Security and Defense*, vol. 41, no. 2, pp. 17–22, 2021, doi: 10.33099/2311-7249/2021-41-2-17-22.

[15] B. Metin, S. Duran, E. Telli, M. Mutlutürk, M. Wynn, "IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture," *Information*, vol. 15, no. 1, 2024, doi: 10.3390/info15010055.

[16] V.L. Buriachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolupa, *Information and Cyber Security: Socio-Technical Aspect*. State University of Information and Communication Technologies, Kyiv, 2015.

[17] Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments.* [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf. [Accessed: Apr. 15, 2023].

[18] ENISA. (Feb. 21, 2023). *Interoperable EU Risk Management Toolbox*. [Online]. Available: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox. [Accessed: Jun. 10, 2023].

[19] D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, CRC Press, Boca Raton, FL, 2021.

[20] N. Yalcin, B. Kılıç, "Information security risk management and risk assessment methodology and tools." International Conference on Cyber Security and Computer Science (ICONCS 2018), 2019. [Online]. Available: https://www.researchgate.net/publication/330170264_Information_Security_Risk_Management_and_Risk_Assessment_Methodology_and_Tools. [Accessed: Jun. 15, 2023].

[21] National Institute of Standards and Technology. (Apr. 22, 2024). *Glossary*. [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: Apr. 15, 2023].

[22] ENISA. (2024). *Glossary of Terms*. [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary. [Accessed: Apr. 15, 2023].

[23] National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Accessed: Apr. 15, 2023].

[24] J. Sokol. (Feb. 25, 2021). *The OWASP risk rating methodology and SimpleRisk*. [Online]. Available: https://www.simplerisk.com/blog/owasp-risk-rating-methodology-and-simplerisk. [Accessed: Jun. 16, 2023].

[25] ENISA. (2022). *Risk management standards: Analysis of standardisation requirements in support of cybersecurity policy.* [Online]. Available: https://www.enisa.europa.eu/publications/risk-management-standards. [Accessed: Jun. 10, 2023].

[26] J. Dobaj, C. Schmittner, M. Krisper, G. Macher, "Towards integrated quantitative security and safety risk assessment," in *Computer Safety, Reliability, and Security,* A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, F. Bitsch, Eds., Turku, Lecture Notes in Computer Science, Springer Cham, 2019, pp. 102–116.

[27] S. Bhamidipati, *Examining approaches to quantifying cyber risk for improved cybersecurity management*, Massachusetts Institute of Technology, 2019. [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/124233/1144933199-MIT.pdf?sequence=1&isAllowed=y. [Accessed: Jun. 20, 2023].

[28] G.-Y. Shin, S.-S. Hong, J.-S. Lee, I.-S. Han, H.-K. Kim, H.-R. Oh, "Network security node-edge scoring system using attack graph based on vulnerability correlation," *Applied Sciences*, vol. 12, no. 14, 2022, doi: 10.3390/app12146852.

[29] O. Korchenko, V. Hnatyuk, E. Ivanchenko, S. Hnatyuk, N. Seilova, "Method for cyber incidents network-centric monitoring of cyber incidents in modern information & communication systems," *Information Protection*, vol. 18, no. 3, pp. 229–247, 2016, doi: 10.5815/ijcnis.2017.06.04.

[30] ENISA. (2022). *Threat landscape methodology*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology. [Accessed: Jun. 10, 2023].

[31] M. Benmalek, "Ransomware on cyber-physical systems: taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, 2024, doi: 10.1016/j.iotcps.2023.12.001.

[32] ENISA. (2018). *Reference incident classification taxonomy*. [Online]. Available: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy. [Accessed: Apr. 29, 2023].

[33] Europol. (2017). *Common taxonomy for law enforcement and the national network of CSIRTs*. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf. [Accessed: Apr. 29, 2023].

[34] ENISA. (2016). *Threat taxonomy*. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. [Accessed: Apr. 29, 2023].

[35] *Threat landscape: Trends and methods. Cyber-threat landscape and end-user requirements*, 31 Aug. 2018. [Online]. Available: https://cyber-trust.eu/wp-content/uploads/2020/02/D2.1.pdf. [Accessed: Jun. 16, 2024].

[36] ZenGRC. (Aug. 10, 2023). *NIST Cyber Risk Scoring.* [Online]. Available: https://reciprocity.com/blog/nist-cyber-risk-scoring/. [Accessed: Aug. 20, 2023].

[37] M. Krisper. (2021). *Problems with risk matrices using ordinal scales*. [Online]. Available: https://arxiv.org/pdf/2103.05440. [Accessed: Jun. 16, 2023].

[38] V. Evrin. (Apr. 28, 2021). *Risk assessment and analysis methods: Qualitative and quantitative*. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods. [Accessed: Jun. 16, 2023].

[39] *About TDR threat scores.* [Online]. Available: https://www.watchguard.com/help/docs/fireware/12/en-us/Content/en-US/services/tdr/tdr_threat_scores.html. [Accessed: Jun. 16, 2023].

[40] S. Ekung, "Limitations of risk identification tools applied in project management in the Nigerian construction industry," *Malaysian Construction Research Journal*, vol. 30, no. 1, pp. 73–85, 2020.

[41] A.N. Kia, F. Murphy, B. Sheehan, D. Shannon, "A cyber risk prediction model using common vulnerabilities and exposures," *Expert Systems with Applications*, vol. 237, 2024, doi: 10.1016/j.eswa.2023.121599.

[42] RiskWatch. (Jan. 31, 2024). *Risk scoring methodology.* [Online]. Available: https://www.riskwatch.com/risk-scoring-methodology/. [Accessed: Jun. 16, 2023].

[43] ENISA. (2019). *EU Cybersecurity Certification Framework: Methodology for sectoral cybersecurity assessments*. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment. [Accessed: Jun. 10, 2023].

[44] C. Borrett, "Threat level index for advanced persistent threats (APT) - European repository of cyber incidents," German Institute for International and Security Affairs, 2022, doi: 10.7802/2494.

[45] T. Mahler, Y. Elovici, Y. Shahar, "A new methodology for information security risk assessment for medical devices and its evaluation," *Computer Science: Cryptography and Security*, 2020, doi: 10.48550/arXiv.2002.06938.

[46] EuRepoC. (2023). *Methodology*. [Online]. Available: https://eurepoc.eu/methodology/. [Accessed: Jun. 16, 2023].

[47] B. Sohval, *A deep dive in scoring methodology*, SecurityScorecard, 2024. [Online]. Available: https://securityscorecard.com/wp-content/uploads/2024/01/EBOOK-MethodologyDeepDive-3.0_v2-1.pdf. [Accessed: Jun. 16, 2023].

[48] J. de Wit, W. Pieters, P. van Gelder, "Bias and noise in security risk assessments: An empirical study on the information position and confidence of security professionals," *Security Journal*, vol. 37, pp. 170–191, 2023, doi: 10.1057/s41284-023-00373-6.

[49] S. Facchinetti, S.A. Osmetti, C. Tarantola, "A statistical approach for assessing cyber risk via ordered response models," *Risk Analysis*, vol. 44, no. 2, pp. 425–438, 2023, doi: 10.1111/risa.14186.

[50] K. Ostrovska, R. Beday, "Productivity study of volume data normalization methods," *System Technologies*, vol. 3, no. 128, pp. 165–175, 2020, doi: 10.34185/1562-9945-3-128-2020-15.

[51] M. Dekker, L. Alevizos, "A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making," *Security and Privacy*, vol. 7, no. 1, 2023, doi: 10.1002/spy2.333.

[52] B. Gokkaya, L. Aniello, E. Karafili, B. Halak, "A methodology for cybersecurity risk assessment in supply chains," *Computer Security, ESORICS 2023 International Workshops*, pp. 26–41, 2024, doi: 10.1007/978-3-031-54129-2_2.

[53] C. Cioaca, C.-G. Constantinescu, M. Boscoianu, R. Lile, "Extreme Risk Assessment Methodology (ERAM) in aviation systems," *Environmental Engineering and Management Journal*, vol. 14, no. 6, pp. 1399–1408, 2015, doi: 10.30638/eemj.2015.152.

[54] P. Nakamura, *Implementing a quantitative risk management methodology in a cyber exercise*, Master's Thesis, JAMK University of Applied Sciences, 2020. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/354191/Masters_Thesis_Nakamura_Petteri.pdf?sequence=2&isAllowed=y. [Accessed: Jun. 19, 2023].

[55] *Science for disaster risk management 2017: knowing better and losing less*, K. Poljanšek, M. Ferrer, M. De Groeve, T. Clark, Eds., Luxembourg, Publications Office of the European Union, 2017.

[56] A.P. Duka, "Risk mapping in the organization's integrated risk management system," *Effective Economy*, no. 10, 2017.

[57] *Threat actors' attack strategies. Work Package 2: Cyber–threat landscape and end–user requirements*, Dec. 31, 2018. [Online]. Available: https://cyber-trust.eu/wp-content/uploads/2020/02/D2.5.pdf. [Accessed: Jun. 16, 2023].

[58] ENISA. (2019). *Online platform for security of personal data processing*. [Online]. Available: https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform. [Accessed: Jun. 10, 2023].

[59] D.W. Hubbard, R. Seiersen, D.E. Geer Jr, S. McClure, *How to Measure Anything in Cybersecurity Risk,* 2nd Edition, New Jersey: John Wiley & Sons, 2023.

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Russia's Invasion of Ukraine and National Cyber Security Strategies: Quantitative Comparison

Olesya Vinhas de Souza | Research Division, NATO Defense College-Rome, Italy | ORCID: 0000-0003-2234-8465

Received: 13.11.2023

Accepted: 20.05.2024

Published: 18.07.2024

Cite this article as:
O. Vinhas de Souza "Russia's invasion of Ukraine and national cyber security strategies: Quantitative comparison," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190346

Corresponding author:
Olesya Vinhas de Souza, Research Division, NATO Defense College-Rome, Italy. E-mail: o.vinhasdesouza@ndc.nato.int;
0000-0003-2234-8465

Abstract

Shared understanding of the operational environment in the cyber domain is the key enabler of NATO's cyber posture. However, there have been no attempts to evaluate empirically the impact of the war in Ukraine on intra-Alliance coherence. This study applies a novel methodology based on computation text analysis to evaluate the trends within the recently adopted national cyber strategies with regards to the description of threats, risks, and actors involved in carrying out these threats – in particular, Italy, Latvia, the United Kingdom, and the United States. The analysis shows that before the large-scale invasion, the congruence was low between the two continental European states vis-a-vis the UK and the US on threat and risk assessment. After the invasion, these differences became smaller and the language of the updated National Cyber Security Strategies became more homogeneous as measured by the cosine similarity scores. There are still differences in the discussion of relevant actors in cyberspace. The methodology applied here can be extended to measure the cohesiveness of the Alliance's cyber posture along other dimensions.

Keywords

cybersecurity, NATO, war in Ukraine, computational text analysis, national cyber strategies

1. Introduction

The ongoing war in Ukraine invigorated scholarly and policy debates about the role of cyber in modern warfare at the strategic and tactical levels because the escalation dynamic did not follow the expected pattern, from cyber to a conventional escalation ladder. Although the intensity of cyber attacks on Ukrainian infrastructure peaked in the early phase of the invasion, to everybody's surprise it was not followed by a cyber Pearl Harbor. In Washington, this subsequently led to the reconceptualisation of cyber from a standalone tool of modern warfare to a critical amplifier of effects across domains. In this process an integrated approach to cyber emerged, particularly in the United States, and most notably was adopted in a recent U.S. Department of Defense 'Cyber Strategy' [1]. At the tactical level, the conflict has been devoid of major changes either in terms of the actors involved or the degree of inter-domain coordination. There seems to be a consensus among cybersecurity experts that the major novelty has been an unprecedented volume of attacks against European NATO members, with a higher share of these attacks accruing on Eastern European and Baltic countries.

This study contributes to the current debate about the effects of the war in Ukraine on the cyber domain by examining whether the Allies moved closer to the shared threat perception in cyberspace since the beginning of the war – the question fundamental for NATO's cyber posture. This study is based on a computational text approach to comparing national cyber strategies for the four Allies that have updated their cyber posture since the beginning of the invasion: Latvia, Italy, the United Kingdom, and the United States. It shows that the saliency of the risk management paradigm vis-a-vis the threat prevention paradigm has increased in some of the European capitals since the invasion and this has subsequently contributed to a greater convergence of threat and risk perceptions within the Alliance. The novel methodology developed in this article can be easily extended to a larger sample to track the internal cohesion within NATO on cyber threat perception as more Allies update their strategies in 2024 and 2025.

The article begins a literature review, and then presents a computational text approach known as cosine similarity. It is based on an analogy with the distance between vectors in Euclidian space and the similarity of the content of the sections of cyber security strategies that focus on the discussion of threats, risks, and actors in cyberspace. The larger the overlap in the vocabulary used in the corresponding sections in the cyber strategies, the greater the convergence within the Alliance on threat perceptions in cyber. The empirical section utilises the fact that cyber strategies are usually enacted for the period of four to five years and thus when countries enact or update their strategies they face a similar threat environments, which may or may not translate into the same cyber posture. So, this study provides a novel empirical approach to evaluating whether the large-scale aggression against Ukraine increased or diminished the consensus within the Alliance. The key finding is that the transatlantic consensus on the key characteristics of the operational environment has increased as a result of new cyber strategies.

2. Literature Review

The rapidly growing open source literature on the cyber dimension of the war in Ukraine can be grouped into (1) tactical studies that have focused on threat environment, types of actors, volume of attacks, geographic distribution of targets, and the types of capabilities used by state and non-state actors and (2) strategic ones that provide a high-level overview of the strategic implications of the cyber capabilities in the future conflicts. The tactical level analysis conducted primarily by think tanks and the IT industry reached the same conclusion that Russia's deployment of cyber capabilities has been haphazard and lacked cross-domain integration as well as cross-actor coordination. It resembled more the activities that were planned and carried out by unconnected networks of non-state actors who did not synchronise their activities with commanders in the theatre. The intensity of these activities picked and ebbed around high-level multilateral events outside Ukraine and the selection of targets outside Ukraine targeted those NATO and EU countries that provided stronger support to Ukraine. Although the geographic scope of the targets surpassed those of the pre-invention level, cyber capabilities have remained the same: DDoS attacks, phishing, malware, ransomware, whispers, hacking, and social engineering [2–9].

One of the unresolved puzzles of the tactical analysis is how in spite of the seeming lack of top-down organisation and/or planning of cyber offensive, the attackers have exhibited a remarkable restraint in the selection of targets outside of Ukraine territory, in such a way not to trigger multilateral or unilateral retaliation by NATO as a whole or some of its Allies. So far, all the ongoing cyber activity has been under the threshold of Article 5 and fortunately has not inflicted either economic or human costs to justify the 'shooting war' that President Biden warned Putin about. It is difficult to reconcile how the fragmented and unconnected attackers managed to calibrate the intensity of cyber offense in a way not to exceed the Article 5 threshold. Subsequently, the large-scale conventional military confrontation broke out in spite of ominous exceptions of cyber Pearl Harbor.

This triggered the reconceptualisation of strategic uses of cyber capabilities particularly in the United States. The unclassified summary of the Department of Defense Cyber strategy published in September 2023 re-conceptualises cyber capabilities from being able to generate strategic effects by themselves to the ones that amplify the effects of capabilities in other domains. Thus cyber should be integrated into other domains to achieve the desired effects. Achieving this goal requires further investment in offensive cyber capabilities as well as extending the cyber toolbox.

The United States was not the only country that has updated its cyber posture since February 24, 2022, the day of the large-scale invasion. The United Kingdom, three EU members – Latvia, Italy, have released new National Cyber Security Strategies (NCSS). Although most of these strategies received attention from the scholarly community in the corresponding country [9–12], there have been relatively few cross-country comparisons of these recent developments [13]. The goal of the analysis that follows is to address this void.

3. Methods

The research design leverages a cutting-edge computational text methodology to compare cyber strategies. Although this is not the first study to rely on computation text analysis, it is the first one to measure the convergence or divergence on a specific issue. For example, Shafqat and Masood [14] and Song *et al.* [15] use latent topic modelling to identify clusters of countries that have similar NCSS. The small sample size in this study (n=10) is the major constraint on directly applying topic modelling here. Therefore, this study instead utilises cosine similarity scoring to compare vocabulary surrounding threats, risks, and actors – the three most contested policy issues when it comes to finding a shared position with the Alliance. By comparing the vocabulary used before and after the large-scale invasion as well as across the four countries, it is possible to assess whether the internal coherence within the Alliance declined or increased since Feb 24, 2022. Cosine similarity scoring was introduced to natural language processing to measure the distance between different texts. Building on an analogy with the distance in Euclidean space, cosine similarity computes a dot product or the angle between two vectors. The values are bounded by 0 meaning that there is no similarity at all between the two texts and 1 means that the two texts are based on identical vocabulary. Words could be arranged in a different order, but two texts consisting of the same vocabulary will get the same scores [16, 17].

4. Results

Before presenting cosine similarity scores, it is useful to highlight the diversity of cyber strategies of continental European Allies (see Figure 1). This figure was produced by the European Union Agency for Cybersecurity (ENISA) to provide a common yardstick for comparing approaches to cyber security within the European Union. It seeks to group strategies based on stated objectives. Although there has been an upward trend in the number of objectives mentioned in cyber strategies, there has been significant variation in the scope of objectives included in them, which makes systemic comparison across countries difficult because of different priorities reflected in the strategies. The objectives range from establishing a rapid response capability to balancing security and privacy and underscore the challenges for systematic comparisons across countries because these objectives are not consistently presented either over time or across the countries.

Therefore, this study focuses on the sentences containing the keywords that appear persistently across the countries and over time: threat(s), risk(s), and actor(s). The extent of similarity or dissimilarity in the vocabulary used when discussing these terms provides insights into the evolution of intra-Alliance coherence over time, especially after the large-scale innovation. Sinc the large-scale invation, only four countries rolled out cyber strategy updates: Italy, Latvia, the United Kingdom, and the United States. The United States updated both the National Cyber Security Strategy issued by the White House as well as the Cyber Strategy published by the Department of Defense. Both of them were included in the study.

Table 1 compares how the discussion about threats, risks, and actors shifted over time. Both the United Kingdom and the United States White House strategies exhibited a high level of consistency over time in the discussion of these terms. This is surprising because of the changes in the administration from President Donald Trump to President Joe Biden. More changes were observed in the DoD strategies, particularly, with respect to risks and actors

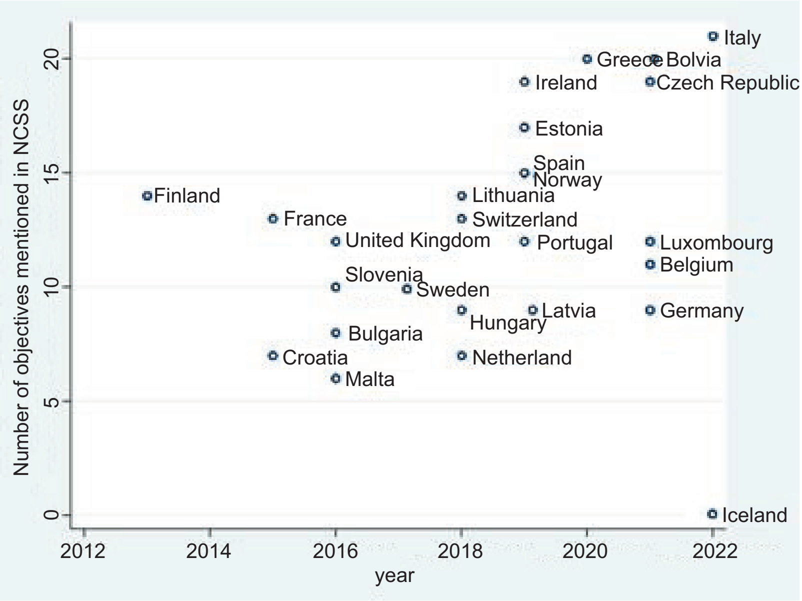


Figure 1. Number of cyber objectives in NCSS increases over time.
Source: Constructed by the Author from ENISA's interactive map available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map. [Accessed: Dec. 20, 2023].

Table 1. Cosine similarity scores before and after the invasion.

	Italy 2017 & 2022	Latvia 2019 & 2023	United Kingdom 2016 & 2022	United States	
				White House 2018 & 2023	DoD 2018 & 2023
Threat(s)	0.49	0.84	0.97	0.92	0.80
Risk(s)	0.58	0.84	0.93	0.89	0.62
Actor(s)	0.48	0.48	0.93	0.83	0.68

Source: Cosine similarity scores were computed by the author using scikit-learn package for Python after extracting sentences with relevant keywords and merging them into text blocks by year and country.

involved. The carryover from the 2017 to 2022 strategy in Italy was comparatively low across all keywords.

Table 2 provides examples of sentences that were analyzed for each keyword for Italy to underscore the fundamental shifts in the complexity of the discussion surrounding the issues. If the 2017 strategy focuses on the concert measures, e.g. National Security R&D Center to deal with the threats, the 2022 focuses on the activities of the Intelligence Community to deal with cyber threats. Although

Table 2. Examples of excerpts from Italy's Cyber Security Strategies.

	2017	2022
Threat	• 'Create a National Cybersecurity R&D Center responsible — among other things — for developing malware analysis, security governance, Critical Infrastructures' protection, threat analysis, etc' • 'National cyber protection and ICT security require an in-depth knowledge of both technological and human vulnerabilities as well as of the threat that exploit them'	• 'The intelligence collection and analysis, aimed at protecting Italy's political, military, economic, scientific and industrial interests, is entrusted to the Intelligence Community, which for these purposes also provides, even though the conduct of cyber operations, for the activities aimed at the detection and systematic monitoring, prevention and contrasting of the most insidious cyber threats perpetrated in or through the digital environment'
Risk	• 'Implementing national cyber risk management' • 'Analysis of costs related to cyber events is a useful baseline for financial planning and allocation of resources, since risk relevance is proportional to event probability and impact'	• 'The risks implied by such complexity – and the potential many economic, social and political implications – range from technological dependence and loss of strategic autonomy of the State to anthropogenic threats, in which human error is added to the initiatives of hostile actors, characterized by different degrees of sophistication and driven by different, but equally harmful, intentions'
Actor	• 'Improving cyber actors' technological, operational, and analytic capabilities' • 'Enlarge and better define the number of actors operating in security relevant sectors' • 'That is why interoperability among actors should be fortified at national and international level'	• 'Beyond the competent institutional actors – which do not end with those mentioned above¹ – this strategy is inspired by a "whole-of-society" approach, which also involves private operators, the academic and research world, as well as civil society as a whole and citizenship' • 'For each measure, associated with the most characterizing goal, the actors responsible for the implementation and all the other subjects involved are indicated, excluding the direct beneficiaries of the measures'

Source: Extracted from Italy's NCSS for 2017–2021 and 2022–2026.

both sentences propose a solution, the language is district. Thus, the computed cosine similarity scores capture well this shift in the context in which these key issues are discussed.

Another peculiar difference between the 2017 and 2022 excerpts is the degree to which risks, threats, and actors are mentioned jointly in 2022 and in completely non-overlapping sentences in 2017. This can be used as an indicator of whether risks and threats are perceived as interchanging or not. Threat mitigation and risk management constitute two fundamentally different approaches to cybersecurity. Threat either exists or not, risk is always there but to a different degree. Threats comprise malign activities of state actors motivated by geopolitical considerations and cyber criminals driven by economic gains. Their activities threaten the interests of the general public and a diverse range of internet users. Resilience to cyber threats emerges as the result of the implementation of comprehensive measures that promote trust and societal awareness. Risk management entails coordinating and integrating across sectors the same approach to risk management, one that takes into account not only the presence of malign actors but also the growing importance of autonomous systems (e.g. AI) that impact both resilience and threat environment in new ways. Risk management requires coordination among different levels of government and sectors. [18, pp. 13–15].

Do the new strategies reflect a greater degree of congruence across the countries on threat and risk perceptions? In the aftermath of the large-scale invasion, both the EU and NATO have enhanced their cyber toolkit to provide assistance to the member states facing cyber attacks, while at the same time homogenising the level of cyber resilience across the Alliance. Table 3 reports cosine similarity scores for each of the countries. The diagonal scores are always 1 because they correspond to the correlation of the country with itself. Therefore, we focus below on off-diagonal terms. Panel A corresponds to the old strategies and Panel B to the updated ones. One of the striking features is that we see greater similarity across all indicators in the new strategies, with only one exception: the differences in the perception of actors between Latvia on the one hand and the UK and US White House strategy increased in the updated versions. Threats are the issue that has the highest level of similarity across the countries whereas actors have the lowest level of similarity. The results also point to the division between the military and civilian approaches to cyber security. The US White House strategy is more similar to the one of the UK rather than to the U.S. DoD’s strategy. Overall, Table 3 suggests that although strategies are becoming longer and more comprehensive in terms of their objectives trans-Atlantic discussions of threats, risks, and actors are becoming more homogeneous. And this is a great news for the Alliance.

5. Conclusions

NATO’s cyber posture has been evolving rapidly since the large invasion along the threat prevention trajectory. The Vilnius summit became a major milestone in this regard. It established an incident response facility to which 11 Allies have already contributed. To avoid the moral hazard problem mentioned above, it also introduced a verification mechanism to ensure that the Allies continue investing in their own cyber capabilities and established ways to enhance private R&D in cyber security by creating the Defense Innovation Accelerator for the North Atlantic (DIANA) funding

Table 3. Cross-country comparison of threat, risk, and actor description.

	Panel A 2016–2021					**Panel B 2022–2023**				
Threat	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.55	1.00				0.89	1.00			
UK	0.50	0.77	1.00			0.89	0.91	1.00		
US WH	0.50	0.77	0.91	1.00		0.86	0.89	0.92	1.00	
US DoD	0.41	0.66	0.82	0.80	1	0.82	0.84	0.87	0.86	1.00
Risk	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.61	1.00				0.89	1.00			
UK	0.57	0.73	1.00			0.87	0.85	1.00		
US WH	0.59	0.75	0.88	1.00		0.85	0.84	0.89	1.00	
US DoD	0.48	0.53	0.75	0.76	1	0.77	0.74	0.76	0.74	1.00
Actor	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.54	1.00				0.66	1.00			
UK	0.60	0.70	1.00			0.79	0.65	1.00		
US WH	0.57	0.67	0.83	1.00		0.71	0.62	0.88	1.00	
US DoD	0.39	0.42	0.56	0.50	1	0.70	0.59	0.86	0.83	1.00

Source: Cosine similarity results were computed by the author using the scikit-learn package for Python, after extracting sentences containing relevant keywords and grouping them into text blocks based on year and country, See Table 1.

mechanism [19]. This is also happening at the same time that the EU level cyber security mechanisms are evolving. The EU’s Strategic Compass adopted in March 2022 seeks to enhance ‘through capacity building, capability development, training, exercises, enhanced resilience and by responding firmly to cyberattacks against the Union, its Institutions and its Member States using all available EU tools.’ It aspires to strengthen the EU strategic autonomy in cyberspace ‘to protect, detect, defend and deter against cyber attacks’ [20].

This is happening at a time when the consensus within the Alliance on the threats, risks, and actors is growing. Although we cannot attribute any causality between these two important trends, we have to be mindful of the importance of common threat perceptions and the assessment of the operational environment in the cyber domain.

This study applied a novel methodology to quantify the trends within the Alliance in the discussion of threats, risks, and actors involved and found that recently adopted cyber strategies point to greater consensus on cyber issues than before the full-scale invasion.

Disclaimer

The views expressed are the author's alone and do not necesseraly reperesent those of NATO or the NATO Defense College.

References

[1] U.S. Department of Defense. (Sep. 12, 2023). *Summary: 2023 Cyber strategy*. [Online]. Available: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF. [Accessed: Feb. 01, 2024].

[2] Cyber Peace Institute. (Dec. 21, 2023). *Cyber dimensions of the armed conflict in Ukraine-Q3,* 2023. [Online]. Available: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/. [Accessed: Dec. 24, 2023].

[3] Digwatch Online Platform. *Ukraine conflict: Digital and cyber aspects.* [Online]. Available: https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects. [Accessed: May 01, 2023].

[4] S. Duguin, P. Pavlova. (2023). *The role of cyber in the Russian war against Ukraine: It's impact and the consequences for the future armed conflict.* [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594. [Accessed: Oct. 17, 2023].

[5] H. Lin, "Russian cyber operations in the invasion of Ukraine," *The Cyber Defense Review,* vol. 7, no. 4, pp. 31–46, 2022.

[6] G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias. (2022). *Cyber operations during the Russo-Ukrainian war: From strange patterns to alternative futures*. [Online]. Available: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. [Accessed: Oct. 02, 2023].

[7] T. Starks. (Feb. 16, 2023). "What we've learned from a year of Russian cyber-attacks in Ukraine," *The Washington Post* [Online]. Available: https://www.washingtonpost.com/politics/2023/02/16/what-we-learned-year-russian-cyberattacks-ukraine/. [Accessed: Feb. 19, 2023].

[8] M. Willet, "The cyber dimension of the Russia–Ukraine war," *Survival*, vol. 64, no. 5, pp. 7–26, 2022, doi: 10.1080/00396338.2022.2126193.

[9] A. Paulus. (Dec. 09, 2021). *German cybersecurity policy*. [Online] Available: https://directionsblog.eu/. [Accessed: Jan. 05, 2024].

[10] F. Oorsprong, P. Ducheine, P. Pijpers, "Cyber-attacks and the right of self-defense: A case study of the Netherlands," *Policy Design and Practice*, vol. 1, no. 23, 2023, doi: 10.1080/25741292.2023.2179955.

[11] A. Jacuch, "Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies," *Modeling the new Europe,* vol. 37, pp. 102–120, 2021, doi: 10.24193/OJMNE.2021.37.06.

[12] J. Neville, "Posturing US cyber forces to defend the homeland," *The Cyber Defense Review,* vol. 8, no. 2, pp. 105–128, 2023.

[13] A. Mishra, Y.I Alzoubi, M.J. Anwar, A.Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, 2022, doi: 10.1016/j.cose.2022.102820.

[14] N. Shafqat, A. Masood, "Comparative analysis of various national cyber security strategies," *(IJCSIS) International Journal of Computer Science and Information Security,* vol. 14, no. 1, pp. 129–136, 2016.

[15] M. Song, D.H. Kim, S. Bae, S.J. Kim, "Comparative analysis of national cyber security strategies using topic modelling," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121209.

[16] A.R. Lahitani, A.E. Permanasari, N.A. Setiawan, "Cosine similarity to determine similarity measure: Study case in online essay assessment." 4th International Conference on Cyber and IT Service Management, Bandung, Indonesia, 2016, pp. 1–6, doi: 10.1109/CITSM.2016.7577578.

[17] D. Gunawan, C.A. Sembiring, M.A. Budiman, "The implementation of cosine similarity to calculate text relevance between two documents." 2nd International Conference on Computing and Applied Informatics 2017 28–30 November 2017, Medan, Indonesia, 2018, pp. 1–6, doi: 10.1088/1742-6596/978/1/012120.

[18] T. Kosub, "Components and challenges of integrated cyber risk management," *ZVersWiss*, vol. 104, pp. 615–634, 2015, doi: 10.1007/s12297-015-0316-8.

[19] NATO. (Jul. 11, 2023). *Vilnius Summit Communiqué* [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_217320.htm. [Accessed: Nov. 14, 2023].

[20] European Commission. (2022). *The Strategic Compass of the European Union*. [Online]. Available: https://www.strategic-compass-european-union.com. [Accessed: Jan. 23, 2023].

Editorial Office

Applied Cybersecurity & Internet Governance
Kolska Street 12
01–045 Warsaw, Poland
www.acigjournal.com

Publisher

NASK – National Research Institute
Kolska Street 12
01–045 Warsaw, Poland
www.nask.pl