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].

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].

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]

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.

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

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].

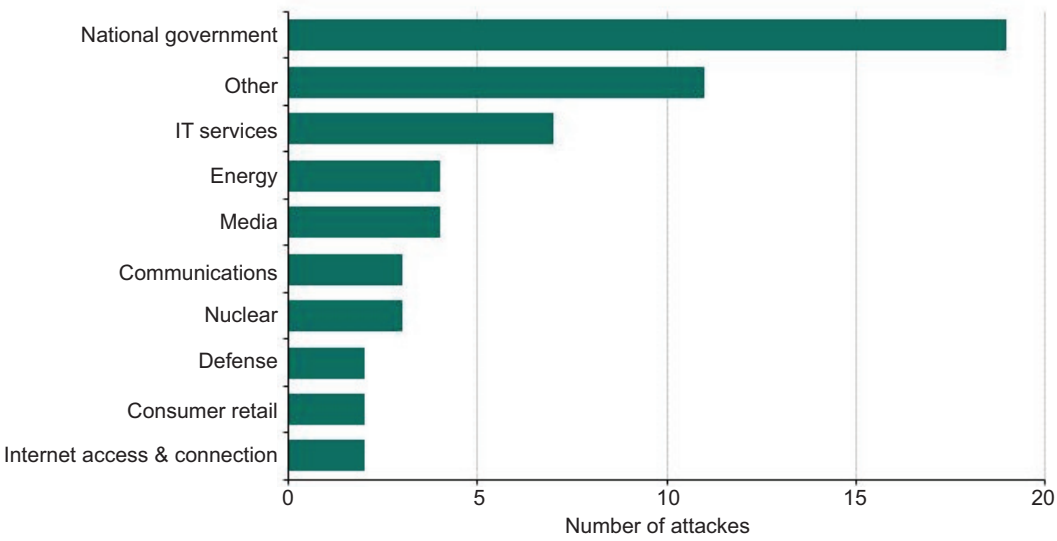

Figure 1. Cyber-attacks on Ukraine by Russia since the invasion began, by sector, July 2022. *Source*: https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine [91].

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].

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

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

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].

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

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

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 disinformation 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-informationwarfare-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). I*ndustroyer: 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-discover-slarge-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].