Opinion
Paper

Visit webpage

Receive Newsletter

99/2022 10/11/2021

*Ada Gavrila**

Ukraine's great cyberwar that did not happen

Ukraine's great cyberwar that did not happen

Abstract:

International society is currently grappling with a hybrid conflict in Ukraine, where traditional and cyber weapons are being used in tandem. The big surprise of the Russian invasion has been the apparent absence of a major cyber war. Russia was supposed to first launch an all-out cyberattack that would cripple Ukraine and set the stage for the physical assault that followed. But this did not happen.

This article explains why Russia has not used the powerful cyber tools it apparently possesses in pursuit of strategic or tactical advantages in Ukraine. Furthermore, it shows how the Ukrainian war may change the traditional parameters of international conflicts through the new configuration of hackers.

Keywords: *cyber security, Russia, cyber warfare, Ukraine, hackers.*

How to quote:

GAVRILA, A. *Ukraine's great cyberwar that did not happen*. Opinion Paper. IEEE 99/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania_ENG.pdf and/or link bie[3] (accessed on the web day/month/year)

***NOTE:** The ideas contained in the Opinion Papers shall be responsibility of their authors, without necessarily reflecting the thinking of the IEEE or the Ministry of Defense.

Introduction

Russia's invasion of Ukraine has disrupted both the real world and the virtual world. However, this is nothing new, as the current war, as it is known, stems from the protracted Russian-Ukrainian conflict that began in 2014, also characterised by Russian cyberattacks on Ukrainian critical infrastructure. Noteworthy are the attack on Ukraine's electricity grid in December 2015, which resulted in a blackout of up to 6 hours for more than 230.000 households[1]; the paralysis of the Ukrainian Treasury in December 2016[2]; and the NotPetya malware attack in 2017[3].

Over the past decade, Russia has increasingly assumed an assertive cyber posture, based on its willingness to conduct cyber operations on critical infrastructure systems, aiming to influence public discourse and create confusion. Moreover, Moscow has repeatedly demonstrated its willingness to employ offensive cyberattacks even in situations other than war, with the aim of affecting political and economic outcomes in other states[4] and ensuring its victory[5].

This article will first analyse the development of the current cyber warfare. Second, it will argue why Russia has changed its cyber strategy. Finally, the impact of the new hacker configuration on future conflicts will be presented.

Development of cyber warfare[6] in Ukraine

Before Russia invaded Ukraine on 24 February, analysts, experts, and officials in several

[1] Available at: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

[2] The cyberattack brought the Treasury's systems to a halt for several days, leaving state workers and pensioners unable to receive their payments. ZINETS, N. Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar', *Reuters,* 2016. Available at: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC

[3] This cyberattack infected a dozen websites of Ukrainian organisations, including banks, ministries, newspapers, electricity companies, and subsequently spread to Germany, France, the United States, and the United Kingdom, among others. HERN, A. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017, *The Guardian*, 2017. Available at https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

[4] The most relevant example is the Russian meddling in the 2016 US presidential election, when Russian cyberattacks contributed to an atmosphere of distrust, polarisation and social fragmentation. This cyberattack not only damaged the victims' chances of winning the election, but also contributed to Americans' already declining faith in democratic institutions.

[5] ORENSTEIN, M. Russia's use of cyberattacks: Lessons from the Second Ukraine War. *Foreign Policy Research Institute*, 2022. Available at: https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks- lessons-

[6] The term ‘cyberwarfare’ refers to the use of information and communication technologies (ICTs) to disrupt the activities of a state or organisation for strategic or military purposes, causing damage comparable to actual warfare. SINGER, P. W. & FRIEDMAN, A. Cybersecurity and cyberwar: *What everyone needs to know*, 2014, pp. 20-22. Available at http://book.itep.ru/depository/cyberwar/P.W.Singer_Allan_Friedman_Cybersecurity_and_Cyberwar_What_Everyone_Needs_to_Know_2014_Oxford_University_Press.pdf

states believed that cyberattacks would play a key role in the war[7]. Specifically, on 22 February 2022, minutes after President Joe Biden announced new sanctions against Russian banks and elites, a senior FBI official called on US businesses and local governments to be mindful of the potential for ransomware attacks as the crisis between the Kremlin and Ukraine deepens[8].

For almost a decade now, Ukraine has become Russia's main victim of cyberattacks aimed at the information systems of its state institutions and private companies[9]. Consequently, it was logical to think that the situation would repeat itself in 2022. In a way, it did happen. During the prelude to the Russian invasion, several cyberattacks against Ukraine were registered.

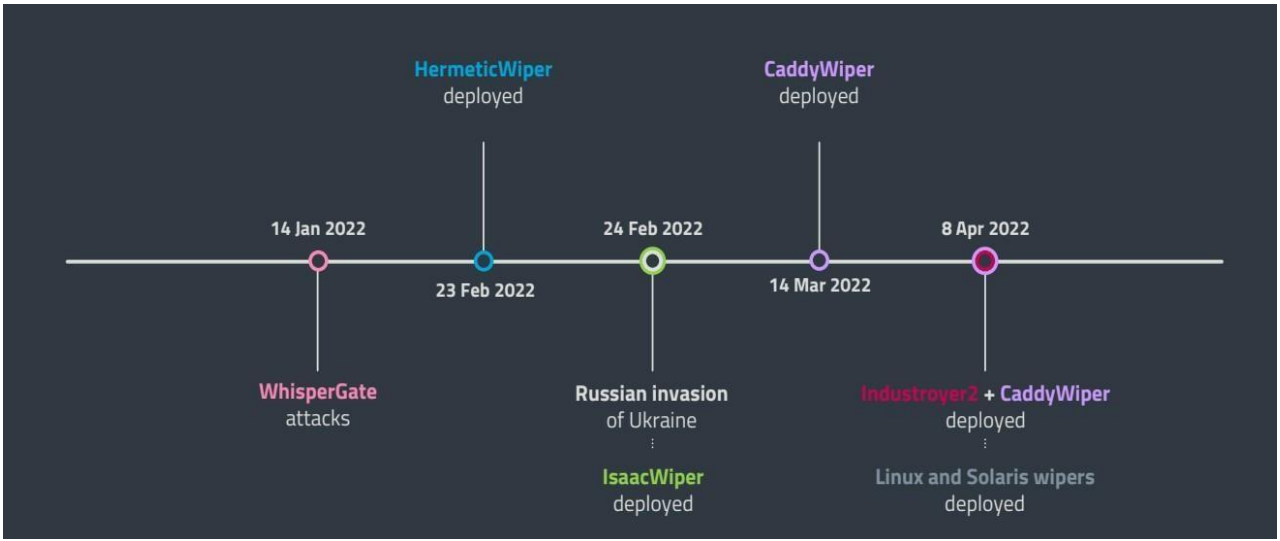

Figure 1. Cyberattacks detected by ESET before and during the invasion. Source: ESET Threat Report[10]

The first cyberattack took place on January 14th and affected around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers and the Security and Defence Council. The hackers replaced the websites with text in Ukrainian, Polish and Russian, which read ‘be afraid and expect the worst’. Most of the sites were

[7] MILLER, C. Throwback attack: Russia breaches Wolf Creek Nuclear Power facility. *Industrial Cybersecurity Pulse*, 24 February 2022. Available at: https://www.industrialcybersecuritypulse.com/facilities/throwback- attack-russian-breaches-wolf-creek-nuclear-power-facility/

[8] LYNGAAS, S. US officials tell businesses to watch for potential ransomware attacks after Biden announces Russia sanctions. *CNN Politcs*, 22 February 2022. Available at: https://edition.cnn.com/2022/02/22/politics/russia-sanctions-fbi-cyber-threats-ransomware/index.html

[9] In 2016, Ukraine suffered the first malware attack specifically designed to attack an electricity infrastructure. PAKHARENKO, G. *Cyber Operations at Maidan: A First-Hand Account in cyber war in perspective: Russian aggression against Ukraine*, 2015, pp. 60-65. Available at: https://web.archive.org/web/20161202005747/https:/ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

[10] Available at: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

restored within hours of the attack[11].

On February 15th, a major distributed denial-of-service (DDoS) attack[12] took down the websites of the Ministry of Defence, the army and the two largest banks in Ukraine, PrivatBank and Oschadbank. The New York Times described it as 'the biggest raid of its kind in the country's history'[13].

On February 24th, an hour before the military invasion, another malicious activity took place, targeting the Viasat-owned KA-SAT satellite network, disrupting internet access in Ukraine and disabling thousands of German wind turbines that used Viasat for communication. Despite having a significant impact, analysts' expectations of a 'major cyberattack' on Ukrainian infrastructure were not met. One of the possible explanations is that two days before the attack the European Union had deployed a cyber rapid response team (called CERT-EU), composed of several cyber security experts[14].

According to ESET's report, the various malware used so far - HermeticWiper, IsaacWiper and CaddyWiper - were targeted at specific (non-)governmental organisations with the aim of affecting their ability to respond adequately to the invasion. ESET identified victims in the financial, government, and media sectors, attributing both HermeticWiper and CaddyWiper to Sandworm[15], a group identified by the US as part of the Russian military intelligence agency GRU.

In addition, on 25 February, organisations and companies such as ESET and Vectra AI considered the possibility of a 'total cyber war' between Russia and the West, because of the unprecedented spate of coordinated cyberattacks in Ukraine prior to the invasion[16]. At the time, cyberattacks had become the weapon of the first attack.

[11] POLITYUK, P. & HOLLAND, S. Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war. *Reuters*. 2020. Available at: https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack- russia-moves-more-troops-2022-01-14/

[12] It is defined as an attack on a computer system or network, with the aim of making a service or resource inaccessible to its legitimate users.

[13] KRAMER, A. Hackers Bring Down Government Sites in Ukraine. *The New York Times*. 28 April 2022. Available at: https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

[14] TIDY, J. Ukraine: EU deploys cyber rapid-response team. *BBC News*, 22 February 2022. Available at: https://www.bbc.com/news/technology-60484979

[15] While some speculated that Sandworm could be a group working out of Russia, it was not until 2020 that the US Department of Justice identified it as Military Unit 74455 of Russia's Main Intelligence Directorate. It is believed to have been responsible for DDoS attacks in 2008 in Georgia and the disruption of Ukraine's power grid in 2015. More information at https://www.cfr.org/cyber-operations/sandworm

[16] ARVANITIS, A. As the War in Ukraine Spirals, Vectra AI Announces Free Cybersecurity Services. *Vectra AI*, 2022. Available at: https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free- cybersecurity-services

A report[17] published by Microsoft in April 2022 shows that most cyberattacks were timed to coincide with incoming missile or ground attacks. The report highlights considerable subtlety in the first weeks of the war, when bombings and troop movements were obvious, but cyber operations were less visible and harder to attribute, at least immediately, to Russian intelligence agencies. In addition, the company concluded that Russia began preparing for Ukrainian cyberattacks in March 2021, at the same time it began deploying troops along its border with Ukraine. The preparatory cyberattacks appear to have been aimed at gathering military and foreign policy intelligence[18] and gaining access to critical infrastructure (especially energy service providers), with the goal of supporting Russian government decision-making and maintaining continuous preparedness of the cyber environment for future contingencies.

In the latest June 2022 report[19], analysts came to two conclusions. On the one hand, two-thirds of Russian cyberattacks launched against Ukraine failed in the first months of the Ukrainian war. Ukraine appears to be well prepared to defend itself against cyberattacks, thanks in part to the work of companies such as Microsoft and Google in moving much of Ukraine's most important systems and databases to the cloud, to servers outside Ukraine. On the other hand, Moscow's disinformation campaign to establish a pro-Russian war narrative is working better than expected. Russia is using disinformation to psychologically manipulate Ukrainian society and reinforce the legitimisation of its invasion. This strategy is well known: Russian military doctrine itself[20] states that information and psychological warfare will largely lay the foundation for victory in the war.

Russia's strategic shift in cyberspace

Based on the above, Russia has not used cyber strategy in the way it was thought it would, any more than the Cyber Pearl Harbor[21] warned about for years. As of February 24th, cyberattacks against Ukrainian systems have been far less damaging than they

[17] Available at https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

[18] As it happened in other conflicts in which Russia has been involved, such as Georgia (2008) and Syria (2011-present).

[19] Available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[20] Available at: https://publicintelligence.net/ru-information-security-2016/

[21] For years, experts have warned that the next war will be fought in cyberspace. A cyber Pearl Harbor would melt government systems, cripple critical infrastructure and plunge modern militaries and societies into darkness. ROHOZINSKI, R. The missing 'cybergeddon': what Ukraine can tell us about the future of cyber war. *International Institute for Strategic Studies*, 2022. Available at https://www.iiss.org/blogs/survival- blog/2022/03/the-missing-cybergeddon-what-ukraine-can-tell-us-about-the- future-of-cyber-war.

could have been. According to ESET's report, the two most relevant attacks have been the CaddyWiper malware attack on March 14th and the Industroyer2 attack on April 8th, both of which were quickly mitigated by the ESET - CERT-EU collaboration.

Thus, Ukraine's critical infrastructure, such as the communications system, energy systems and healthcare systems have suffered more from direct military attacks than from cyberattacks. This is very surprising since, when Russian forces invaded Crimea in 2014, they had already shut down Crimea's telecommunications infrastructure, disabled most Ukrainian websites and blocked the mobile phones of several Ukrainian officials[22].

There are three main arguments for Russia's strategic shift in cyberspace.

First, according to Lauren Zabierek[23], the main reason is that Russia wanted to avoid an escalation of tensions with third states or spillover effects beyond Ukraine[24]. Specifically, it has tried to prevent a spillover effect from cyberattacks that could trigger a cyberwar with the West. No state has an interest in provoking a global cyber war, not even Russia - especially in a context in which its economy is severely weakened. It is also very likely that the war has created a kind of *détente*, where both sides understand that catastrophic cyberattacks will result in the mutually assured destruction of their critical infrastructures.

Moreover, Putin's intention has been to avoid invoking article 5 of the North Atlantic Treaty[25] especially after the organisation updated its Strategic Concept at the Madrid Summit in June 2022. If the previous version[26] from 2010 briefly stated the rise of cyberattacks against the West, the new document[27] directly accuses Russia of using malicious cyber operations as well as a disinformation strategy against the Allies to 'establish spheres of influence' and 'pursue its political objectives of undermining the international order'. Russia also becomes the most significant and direct threat to the Alliance.

The second argument is that since cyber operations did not provide Russia with an

[22] European Union External Action. *Eight Years On, War in Ukraine Brings Back Painful Memories of Crimea's Invasion*, 2022. Available at https://www.eeas.europa.eu/eeas/eight-years-war-ukraine-brings-back-painful- memories-crimea%E2%80%99s-invasion_en

[23] Cybersecurity expert and Executive Director of the Cyber Project at Harvard Kennedy School.

[24] Available at https://www.nature.com/articles/d41586-022-00753-9

[25] As explained by CUBEIRO CABELLO, E. in *El ciberespacio en la guerra de Ucrania*. Documento de Opinion IEEE 32/2022. Available at https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf

[26] Available at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic- concept-2010-eng.pdf

[27] Available at https://www.nato.int/strategic-concept/

operational advantage in 2014, so Moscow prioritised military rather than cyber actions[28]. Cyberattacks are not yet effective as tools of coercion in warfare, as they have so far failed to have a discernible effect on violence in the physical world[29]. Although increasingly common, cyber operations in wartime are not as useful as bombs and missiles when the objective is to inflict physical and psychological damage on the enemy. Simply put, an explosive payload causes more long-term damage than a malicious piece of software.

Likewise, cyberwarfare cannot replace traditional forms of warfare. States will not use cyberwarfare in place of traditional warfare, but they will increasingly rely on cyberspace as a domain in which to pursue new information objectives[30].

Finally, there is the third and most plausible argument - states' desire to increase their cyber-defence capabilities has become more important in recent years. Ukraine is the best example. Over the past eight years, Ukraine has survived massive Russian attacks on its critical infrastructure, as well as a wave of destructive malware - NotPetya - and these lessons have been vital for the Ukrainian government, which has strengthened its resilience and response capacity. In the current context, Ukraine's cyber defences were augmented by foreign assistance[31]. As a result, Ukraine continues to maintain a high level of operability and connectivity, thanks, in particular, to the massive investment[32] to establish a satellite internet service in the country, operated by SpaceX.

However, some experts suggest that Russia may be keeping its most aggressive cyber weapons in reserve. If the ground war stalls and financial sanctions hit it too hard, Moscow will increase cyberattacks towards Ukraine, or could even target international companies

[28] ISHAK, N. Is Russia holding back from cyberwar? *Vox*, 19 March 2022. Available at: https://www.vox.com/2022/3/19/22986316/russia-ukraine-cyber-attacks-holding-back

[29] KOSTIUK, N. & ZHUKOV, Y. Invisible Digital Front: Can Cyberattacks Shape Battlefield Events? *Journal of Conflict Resolution,* 2017. Available at https://web.archive.org/web/20220316084344/https://journals.sagepub.com/doi/10.1177/0022 002717737138

[30] Cyber warfare is first and foremost about information: its control and use to achieve political objectives. As primarily an informational domain, cyberspace is more useful for pursuing informational objectives and psychologically manipulating the target society than for winning a war. KOSTYUK, N. & GARTZKE, E. Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine, *Texas National Security Review*, 2022. Available at: https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark- loudly-in- russias-invasion-of-ukraine/

[31] For Cubeiro Cabello *(op. cit.)*, the actions of states, particularly the US, are fundamental. The US Cyber Defence Command and the US Agency for International Development have considerably reduced the vulnerabilities of Ukrainian essential services and critical infrastructure, strengthening its capacity to prevent and mitigate cyberattacks.

[32] According to various sources, the US government has spent around $800,000 to establish the service, delivering more than 5,000 terminals to the Ukrainian government. COLLIER, K. Starlink internet becomes a lifeline for Ukrainians. *NBC News*, 2022. Available at: https://www.nbcnews.com/tech/security/elon-musks- starlink-internet-becomes-lifeline-ukrainians-rcna25360

and financial markets[33]. In this regard, it is worth noting that although most of Russia's cyber activity has focused on Ukraine, Microsoft has detected 128 network intrusions in 42 countries[34]. Thus, Ukraine is not the only state to have been the victim of cyber-attacks since the beginning of the war. Intrusions have been detected in Spain[35], Germany[36], and the United Kingdom[37], among others.

Hackers at war

One of the most interesting components of the Russian-Ukrainian cyber war is that states are not the only actors, but that each side is supported by various cyber groups. Ukraine received support from hacker groups such as Anonymous, Ghostsec, or the Belarusian Cyberpartisans, while on the Russian side are the Conti, Free Civilian and Killnet groups, among others.

In addition, Ukraine pursued a unique cyber strategy in the conflict: on 26 February the government announced the creation of a "volunteer cyber army" to protect Ukraine's critical infrastructure, conduct cyber espionage missions against Russian troops, as well as attack Russian military targets. So far, hacktivists managed to delete many CIS files, rename hundreds of folders to ‘putin_stop_this_war’ and expose email addresses and administrative credentials of members of the Russian government. In addition, out of 100 Russian databases that were analysed, 92 had been compromised by hackers[38]. Yurii Shchyhol, head of Ukraine's State Service for Special Communications and Information Protection acknowledged the importance of the hacktivists' work: by providing information

[33] GIBNEY, E. Where is Russia’s cyberwar? Researchers decipher its strategy, *Nature*, 17 de marzo de 2022. Available at https://www.nature.com/articles/d41586- 022-00753-9

[34] For more information, see https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[35] Since the invasion, the sending of dangerous emails by Russian groups to the main Spanish press, radio and television media has increased by 3,000%, reaching peaks of more than 4,000% since 1 March. AGUIRREGOMEZCORTA, M. El otro campo de batalla: se intensifican los ciberataques rusos a las empresas españolas, *NIUS Diario*, 4 March 2022. Available at: https://www.niusdiario.es/ciencia-y- tecnologia/tecnologia/otra-guerra-ciberataques-rusos-alcanzan-empresas- espanolas_18_329202222292.html

[36] In May 2022, Killnet, a group of pro-Russian hackers took down the websites of the German Ministry of Defence, Parliament, the Federal Police and several local police authorities. Gebauer, M., Röbel, S., Rosenbach, M. & Wiedmann-Schmidt, W. Putin-Fans attackieren deutsche Behördenseiten, *Der Spiegel*, 2022. Available at: https://www.spiegel.de/politik/deutschland/killnet- cyberangriffe-wladimir-putin-fans-attackieren-deutsche-behoerdenseiten-a-2be17f20-3688-4674-b82d- d7889a532c8

[37] One in three UK businesses reported that they were experiencing cyber breaches or cyberattacks at least once a week. GOV.UK. Businesses urged to boost cyber standards as new data reveals nearly a third of firms suffering cyberattacks hit every week, 2022. Available at: https://www.gov.uk/government/news/businesses-urged-to-boost-cyber-standards-asnew-data-reveals-nearly-a- third-of-firms-suffering-cyber-attacks-hit-every-week.

[38] DELCKER, J. Ukraine's IT army: Who are the cyber guerrillas hacking Russia? *Deutsche Welle*, 24 March 2022. Available at: https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a- 61247527

to government institutions on how to properly defend critical infrastructure, none of the cyberattacks allowed the enemy to destroy any databases or cause a leak of private data[39]. However, these groups should be cautious, as aiming at the wrong target or conducting a disproportionate operation can create additional tension.

The establishment of hacker groups on both fronts led Clarke[40] to determine that the war in Ukraine is changing cyber groups' decision-making in terms of recruitment. Prior to the war, cyber mercenaries were configured as apolitical groups, often motivated by money, disruption of critical infrastructure, or some vague affiliation with a cause. However, the current context is different. If these groups were previously driven by the proceeds of ransom payments, they are now being deployed in armed conflict for the sake of their country or a country with which they feel solidarity. Previous rules among hacker groups in the region are eroding, dividing the groups along conflict lines[41]. In short, hackers are pitting themselves against each other in support of or against Russia. As cyberattacks and conflict continue, these deepening divisions on the two fronts are a defining change for future conflicts.

On the Russian front, the fragmentation of groups[42] and the lack of agreed standards in the future mean that recruitment modalities will change. Instead of accepting someone with cyber expertise to carry out attacks, these groups might begin to require a certain 'political loyalty' to be maintained for admission.

The motivation for cyber-attacks is also changing – it is no longer only intellectual or economic, but also political, so that the consequences are no longer focused solely on economic loss, but on conflicts between states, which also demonstrate and measure their strength in cyberspace.

On the Ukrainian front, the government has expressed its support for the volunteer cyber army but has also made it clear that it is not working in unison with them[43]. This is the first

[39] ROSEN, K. The Man at the Center of the New Cyber World War. *Politico*, 14 July 2022. Available at: https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486

[40] CLARKE, A. Hacking the Invasion: The Cyber Implications of Russia's Invasion of Ukraine. *Third Way*, 7 June 2022. Available at: http://thirdway.imgix.net/pdfs/hacking-the-invasion-the-cyber-implications-of- russias- invasion-of-ukraine.pdf

[41] Accenture. *Global Incident Report: Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums*, 2022. Available at: https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf

[42] For instance, in May 2022, the pro-Russian cyber group Conti announced the end of its operations, after officially eliminating its attack infrastructure and dividing its malicious cyber activities to other smaller groups.

[43] JASPREET, G. Why Ukraine recruiting amateur 'IT army' could backfire. *Breaking Defense*, 2022. Available at: https://breakingdefense.com/2022/03/why-ukraine-recruiting-amateur-it-army-could-backfire/

time in Ukrainian history, and probably in world history, when nearly 300,000 volunteer cyber professionals are coordinating their efforts to plan and execute any attack on Russian cyber infrastructure without state backing. They do it on their own. While the Ukrainian government may express concerns or objections to certain ‘tasks’ of the group, there is nothing to prevent the group from carrying out an attack without its approval or for the group's offshoots to act outside of the established targets.

Conclusions

Russia has traditionally been very active in cyberspace, which is why one of the most widely held beliefs among experts is that its cyber capabilities are very extensive. In practice, however, there has been a gap between how states and doctrine thought Russia would act in the cyber war against Ukraine and what has actually happened.

The combination of kinetic attacks with cyberattacks in hybrid warfare generally seeks to overwhelm enemy decision-making; create social unrest and polarisation; or paralyse critical infrastructure such as government services, energy, finance, and transportation. Russia has not achieved any of these objectives so far.

Moreover, Russia's cyber strategy has not been at all effective compared to the one used for the annexation of Crimea in 2014. This is mainly because Ukraine's defensive cyber capabilities are not the same as they were eight years ago, as well as the support of several states, companies such as Microsoft and Google, and, above all, hackers such as Anonymous or the volunteer cyber army.

The great novelty of the war is the new role of non-state actors – for the first time in history, anyone can join the war. If, in the future, hacking groups demonstrate that they do not need state support to operate, the real ability of a state to control malicious activity on its territory will become increasingly limited. Even in the absence of conflict, external hacking groups could begin to form for purely political reasons. This implies that, in future conflicts, it may be states themselves that will need external actors to support their cyber activities against their adversary.

While the *Cyber Pearl Harbor* that was expected to be seen in the first major clash between advanced industrial states in the 21st century has not happened, this may be changing. Uncertainty about Russia's duration and destructive capabilities will continue to change the dynamics of the conflict and could alter the way the cyber component of the conflict is currently playing out. While the 'total' cyber war of this conflict has not emerged, its impact on different areas of cyber security will be felt in future conflicts. Already since the start of the war, numerous states have reported an increase in Russian cyber-attacks on their infrastructure.

It is therefore absolutely necessary for international peace and security that the West prioritise a coherent cyberdefence strategy and increase investment in defensive (and perhaps offensive) cyber capabilities in order to respond adequately to threats from cyberspace.

Although the cyberwar in Ukraine did not occur as expected, it has played an important role from the outset, marking the existence of two challenges for international society. On the one hand, to understand under what circumstances cyberwarfare might or might not occur in future conflicts; and on the other hand, faced with the challenge of the new hacktivists, to determine to what extent states remain the only actors that control cyberspace.

*Anda Gavrila***
Political Scientist from the University of Granada
Delegation of the Junta de Andalucía in Brussels
@ada_gavrila