Eurodefense, Portugal

The dynamics of conflicts in Cyberspace

CMG Helder Fialho Jesus
Jesus.hmf@ium.pt

1. Introduction

The intention of this document is to provide a reflection of the actual wars in Ukraine and in Gaza, focusing on the cyberspace. Actors, support provided, and events are part of this paper. As the Ukraine war is longer than the Gaza war, and with different interests, more information is provided regarding the former.

2. Ukraine

With the annexation of Crimea in 2014, the Russia-Ukraine conflict has been a significant political issue, with consequences in cyberspace. Since then, the US has been playing a significant role in Ukraine's foreign policy, supporting several significant reforms there and influencing international institutions, among them, the North Atlantic Treaty Organization (NATO) and the International Monetary Fund (IMF). In 2017, a US-Ukraine Bilateral Cyber Dialogue was established to strengthen national response planning, infrastructure security and information sharing, linking Ukraine with the US Defense, Energy and Treasury departments. In the last years before the Russian invasion in February 2022, Ukraine has participated in multinational exercises in cyberspace with NATO and other NATO allies.

To understand the conflict in the cyberspace domain, the “UNICEF Guide to Conflict Analysis” and the “Guidance note on the use of conflict analysis in support of EU External Action” were followed, focusing on the effects (the Branches of the Tree). To have a holistic view in the cyberspace in this war, it is important to know the cyber capabilities of the parts in conflict, through trustworthy indexes like the Global Cybersecurity Index (GCI). This is issued by the International Telecommunication Union (ITU), the United Nations (UN) specialized agency for digital technology and evaluates the countries' cybersecurity commitment toward a secure digital ecosystem, considering five pillars. The USA ranking first, Russia fifth, and Ukraine as the 78th country with capacity development as the weakest pillar. All the UN member states are committed to the United Nations' norms of responsible state behaviour in cyberspace with the Open-Ended Working Group (OEWG) on Information and Communications Technologies. Its approved report, published in March 2021, contains 11 voluntary and non-binding rules describing what states should and should not do in cyberspace.

Ukrainian cyberspace has been studied with different views, including the academic, the military and political perspectives. These include the cybersecurity system and the information warfare environment in Ukraine. Noteworthy are the 2015 and 2016 winters, when Ukrainian power grids were victims of disruption by proxy groups linked to Russia, which left a quarter of a million people in darkness and with great impact in the society, due to the absence of energy for several hours. In 2017, the Notpetya malware, originating in Russia caused losses of over $400 million and paralyzed a third of Ukraine's economy for three days. It also caused $10 billion in damage worldwide and was considered as the "most destructive and expensive cyber-attack in history. This malware affected companies worldwide including WPP, Merck and Maersk, amongst others, the latter with a loss of almost $300 million.

Looking to the Russian's view on cyberspace, it can be divided into two levels: external, focusing on the Western public and decision-makers; and internal, focusing on Russia's efforts to ensure independence from the global Internet network. Russia sees cyber operations as an increasingly significant tool in the ongoing "information confrontation", which leads the NATO STRATCOM COE to consider that Russia explores the cyberspace within a broad definition of the information domain, including both technical and psychological components. The digital transformation represents a world economy's objective for a future sustainability development, and it is also part of the Moscow objectives to cyberspace. But numerous issues are preventing it from fully digitalizing, such as technical private companies including Google, Microsoft, PayPal, IBM, and CISCO leaving Russia due to the actual war.

Cyberspace security is also a European concern, with the EU Cybersecurity Agency (ENISA) providing annual reports on the status of cybersecurity threats. This war between Russia and Ukraine has reshaped the threat landscape, with geopolitics having a more substantial impact on cyber operations.

Interesting to note: the Ukrainian diaspora includes over 1 million Americans with Ukrainian ancestry and 20,000 Ukrainian immigrants living in California. Many of these immigrants work in Silicon Valley, which highlights the strong relations between the US and Ukraine and the technological affinity.

Since the Maidan events in 2014, Ukraine's tech sector has grown rapidly, creating a new class of young, wealthy workers with deep ties to the West. But also with this event, the hybrid threat environment increased in Ukraine, with manipulative and unwanted interference in the society through various tools, including disinformation, historical narratives, election interference, cyberattacks, and economic leverage. The term "hybrid war" has become more familiar in the media environment, with articles in several occidental magazines highlighting the growing influence of Russia's hybrid activities against Ukraine. Following the recent invasion of Ukraine, Russia's cyberattacks have accelerated dramatically, namely with wiper malware to destroy the data, threatening the Ukrainian internet and endangering vital information, services, and infrastructure.

The present reflection was conducted in the timeframe from October 2022 to February 2024. It considers the international support to Ukraine in cyberspace as the object of study and uses a qualitative research strategy based on a literature review. This analysis does not consider the dimensions of (dis)information and psychological warfare in cyberspace, and is based in western and Ukrainian sources, providing therefore a non-global view of the facts needed for an independent analysis.

3. Institutional Support to Ukraine – Countries, Organizations and Companies

The international support to Ukraine has grown significantly since the invasion of Crimea in 2014, with the cyberspace being part of it. Reports from the European Parliament show that Ukraine has suffered the most from cyber-attacks since 2014, including phishing emails, denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves. A Carnegie Endowment for International Peace report evaluates the international support to Ukrainian in the context of cybersecurity, stating that a significant rise in capabilities and capacity has been achieved due to the worldwide effort to support Ukraine. A report of the Science and Technological Committee of the NATO Parliamentary Assembly provides an interesting view on four technological areas in this conflict, namely the satellites, drones, mobile phone cameras, and cyberspace.

This document divides the support to Ukraine in cyberspace in two moments: before and after the February 24, 2022, along with a note to the hacktivism.

a. Before the invasion, some activities of the US should be highlighted: The FBI provided Ukrainian partners with direct support in law enforcement, assisting against disseminating disinformation, disrupting nation-state efforts, and exchanging investigative techniques on cyber incidents. Since 2017, the US Department of State has provided Ukraine with $40 million in cyber development assistance, and in 2020, it announced an additional $8 million in cybersecurity support. Between December 2021 and March 2022, US Cyber Command joint forces collaborated with the Ukrainian government to enhance cyber resilience in national critical networks. With around 40 US troops, the mission became one of its largest deployments, focusing on detecting harmful online activity on Ukrainian networks.

   Regarding International Organizations, the NATO support to Ukraine has two dimensions: capability development, through the NATO-Ukraine Cyber Defence Trust Fund, which created laboratories as well as an incident management center and technology support, with the access to the NATO's Malware Information Sharing Platform (MISP), to facilitate the information sharing on technical aspects of malware within the Allied community. On the European Union (EU) side, the most notable support is the €25 million project to aid Ukraine in its digital transformation and integration with the EU Digital Single Market. The Estonian E-Governance Academy has successfully carried out complex e-government projects in Ukraine since 2012. Coincidently, few days before the invasion, the EU Cyber Rapid Response Teams (CRRTs), a project developed within the EU's Permanent Structured Cooperation (PESCO) framework to respond to cyber incidents, were activated to help Ukraine's institutions in cybersecurity.

b. After the invasion, it is notable that there was a great support by the western private sector of cybersecurity on Ukrainian companies and governmental institutions. Several companies like Vectra AI, Avast, CrowdStrike, Cloudflare, CISCO and Palantir have offered services for network infrastructure scanning, endpoint protection, and security solutions as well as artificial-intelligence software to support Ukraine's defense. But Amazon, Microsoft, and Google, as part of the five big technological companies, known by the acronym of GAFAM, should be more addressed due to their global market value and support for Ukraine.

   Amazon Web Services (AWS) has been instrumental in safeguarding crucial data in Ukraine's banking, educational, and government sectors. In February 2022, the same month of the Russian invasion, Ukrainian law was changed to allow the transfer of public and private sector data to the cloud, which belongs to private companies. After a Ukrainian government public plea for assistance to achieve that, the AWS was one of the first firms to respond, securing, storing, and moving data to the cloud. Since the beginning of the war, Amazon has provided over $45 million in resources, goods, and cloud computing credits to local charities, and AWS has pledged $15 million in cloud computing credits and technical help. AWS has also supported Ukraine in migrating state registers and other vital state databases to the AWS cloud environment.

   Microsoft has introduced AI solutions to combat cybercriminals and protect clients' online activities. In response to the war in Ukraine, Microsoft reduced its business in Russia and pledged $100 million in technical assistance to Ukraine during the Lisbon Web Summit 2022, increasing its overall funding to over $400 million since the war began, in February. Through 2023 to 2024, Microsoft continued to provide Ukraine with free technology support. The company's Special Reports on Ukraine provide insights into Russia's use of cyber capabilities and offer strategic recommendations to organizations worldwide. In 2022, three reports were issued, providing strategic and technical details. The first report, "An overview of Russia's cyberattack activity in Ukraine," assessed the climate of urgency and warned of restricted capabilities like zero-days, attacks on infrastructure, and supply-chain attacks. The second report, "Defending Ukraine: Early Lessons from the Cyber War," highlighted the cyber components of the ongoing conflict and the unique characteristics of cyberspace. The last 2022 report,

“Preparing for a Russian cyber offensive against Ukraine this winter”, issued in December, warns of a Russian cyber offensive against Ukraine, aiming to pressure domestic and international sources of support, initiating a hybrid campaign.
Google, the most popular website and search engine globally, has increased security measures to protect Ukrainian civilians and websites following the invasion. The company's President of Global Affairs, Kent Walker, announced measures such as SOS alerts, automated detection, Gmail notifications, increased authentication challenges, and the expansion of Advanced Protection and Project Shield programs. The Google Threat Analysis Group (TAG) is supporting in defence against sophisticated threats and state-sponsored malware attacks. Since Google acquired Mandiant, the company leader in Threat Intel and investigation in incident response services, it is providing better cybersecurity services to its customers and, consequently, to Ukraine.
In February 2024, Time magazine dedicated an edition to the “How Tech Giants Turned Ukraine Into an AI War Lab”, where Steve Blank, a tech veteran and co-founder of the Gordian Knot Center for National Security Innovation at Stanford University states that “This is the first time ever, in a war, that most of the critical technologies are not coming from federally funded research labs but commercial technologies off the shelf,” “And there’s a marketplace for this stuff. So, the genie’s out of the bottle.”

With a different approach, a special word must be given to **Starlink,** SpaceX's satellite network. This big private company, not IT but using the cyberspace in its processes, aims to provide internet access to all of the Earth, especially to isolated areas. This enterprise has been enabling many Ukrainians, including the military, to stay online, despite power outages and Russian attacks on Ukraine's internet infrastructure. It is a secure satellite system and easy to use, with the installation taking only 20 minutes. Over 25,000 Starlink terminals have been delivered to Ukraine from foreign partners, volunteers, or directly from SpaceX. The Starlink network has helped Ukraine to win the drone war in the beginning of this conflict, as the Ukrainian military uses the "Delta" technology to locate and destroy invading forces. Ukrainian soldiers could use drones to relay data to Command and Control (C2) centers and organize strikes against Russian military troops. The Delta, a situational awareness and battlefield management system developed and used in *Ukraine*, has been tested at the Sea Breeze military exercises, in the Black Sea. This is a series of multinational maritime exercises, led by the USA, to improve interoperability with NATO systems. Without Starlink's early and cheap access, Ukrainian networks could not have survived.

Some International Organizations have also providing/continued to provide support to Ukraine. The **NATO** support in cyberspace includes the admission of Ukraine to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2022. The CCDCOE provides interdisciplinary expertise in technology, strategy, operations, and law. Regarding the support with cyber threat intelligence or other kind of information, it can be considered as part of the NATO position in this conflict. By its side, the **EU** has invested over 10€ million in Ukraine to enhance cybersecurity and maintain public services, with the "EU Support to Strengthen Cyber Security in Ukraine" project in 2022. Next year, more 17,4€ million to the project “Digital Transformation for Ukraine (DT4UA). The European Union Agency for Cybersecurity (ENISA) has formalised a Working Arrangement with Ukraine counterparts focused on capacity-building, best practices and situational awareness.

Considering the support provided by countries, two can be underlined: the **US,** that has added $45 million to Ukraine's cybersecurity defense in 2022, enhancing its cyber defensive capabilities. The Cybersecurity and Infrastructure Security Agency (CISA) signed a Memorandum of Cooperation with the Ukrainian State Service of Special Communications and Information Protection of Ukraine to provide warnings preventing malware targeting of Ukrainian enterprises. In the intelligence services, the US has also been actively disclosing Indicators Of Compromise (IOCs) from Ukrainian networks, serving as digital forensics for network defenders and proof of Russian intrusions. And the **UK**, with the Ukraine Cyber Program, funded by £6.35 million, which aims to protect Ukraine's government and infrastructure from cyberattacks following Russia's invasion. The program, involving industry collaboration, aims also to prevent malicious actors from accessing key networks.

c. In the Ukrainian side of strategic decisions, the volunteer IT Army to fight Russia online, is an example, targeting railways, energy grid, and governmental and financial institutions. This army, which has thousands of cybersecurity professionals, is part of the "digital war" against Russia. The number of IT Soldiers is unknown, but by the end of February 2022, 175,000 people had subscribed the public channel provided by the Ukrainian government. The IT Army volunteers have different motives, expertise, and abilities to use cyber weapons. Anonymous is a powerful player in Ukraine's cyber guerrilla army, with hacks on over 300 Russian cyber targets in 48 hours. However, Tim Stevens, a senior lecturer in global security at King's College London, warns of unexplored and hypothetical scenarios when it comes to cyberattacks and the possibility of escalation. Another apprehension is with cybercrime, with the world of cyber criminals currently divided between supporters of Russia and Ukraine. Rob Joyce (NSA-USA) and Lindy Cameron (NSCS-UK) have alleged that Western nations are concerned about the resurgence of hacktivists.

To close this theme, and taking in consideration reports from the International Institute for Strategic Studies (IISS), Chatham House (CH), European Parliament (EP), Carnegie Endowment for International Peace (CEIP), the European Cyber Conflict Research Initiative (ECCRI) and the Center for Strategic & International Studies (CSIS), some key takeaways/extracts can be presented:

- The fundamental goals of wartime operations—sabotage, influence, and espionage—have remained unchanged (ECCRI).
- Ukraine has successfully resisted Russian cyberattacks thanks in large part to assistance from its international allies as well as—and this is crucial—the private sector (CH).
- Due to their significant engagements in the conflict, digital corporations have been highlighted as geopolitical actors as a result of the war: these companies' direct offering of cyber-security services and capabilities has supported Ukraine's cyber defense during critical times; and due to their withdrawal from Russia after the invasion, tech corporations have damaged Russia's economy and prestige (IISS).
- Russia launched a persistent effort to breach and interfere with Ukraine's vital national infrastructure, but defense dominated the majority of the effort since it had access to excellent intelligence and world-class cyber-security knowledge (IISS).
- The incapacity of Russia to coordinate cyber operations with other military impacts, the poor state of its own cyber security, and the absence of the skills necessary to surgically disable military combat targets are the main shortcomings in Russian cyber capabilities when compared to those of the US (IISS).
- It is getting more and more difficult to differentiate political activist groups from cybercriminals, what undermines the notional protection they are afforded as civilians rather than combatants (CH).
- The (Cyber) Confrontation will not finish with a ceasefire (CEIP).
- In large theatre wars, cyber activities will be supportive rather than decisive (CSIS).
- War will continue to be a tool of advancing politics, depending more on the visible results of bloodshed than on the less obvious consequences of breaking into communication networks (CSIS).

- Because they enable a non-violent engagement that uses covert action, propaganda, and monitoring in a way that fundamentally threatens human rights, cyber operations continue to be valuable as a tool of political warfare. Cyber operations will remain a limited tool of coercion (CSIS).

4. Gaza

Moving now to the actual conflict in Gaza, where the Israel is in war with Hamas, in cyberspace it worthily to mention two reports issued in February 2024. One by Google Threat Analysis Group and Mandiant based in operations by six regional threat groups with ties to Hamas, Hezbollah, and Iran. The main activities conducted were in cyber espionage, information operations, and potentially destructive activities. In this case, the cyber operations did not play a supporting role like they did in the beginning of the Russian offensive in Ukraine, being used independently. Iran, a long-standing adversary of Israel and the US, continues its cyber operations. In the six months leading up to the Hamas attack, Iran was responsible for about 80% of government-sponsored phishing activity targeting Israeli users.

The other report, by Microsoft Threat Analysis Center (MTAC), highlighted that Iran has conducted cyber-enabled influence operations in support of Hamas during the Israel-Hamas war. These operations combine offensive cyber activities with messaging to shift perceptions and behaviors. Three phases could be considered: (1) Reactive and Misleading: Initially, Iranian groups were reactive, exaggerating the scope and impact of claimed cyberattacks, however there’s no clear evidence of coordination with Hamas before the October 7 attack; (2) Targeted Influence Tactics: Iran’s influence operations have sought to intimidate Israelis, criticize the Israeli government, and undermine support for Israel’s military operations and (3) Growing Threat: As the conflict persists, Iran’s cyber and influence operations are expected to escalate, especially amid the potential for a widening war. Note: a Gaza-based threat actor known as Storm-1133 has targeted Israeli private-sector energy, defense, and telecommunications organizations.

Also noteworthy: the news report of a US cyberattack launched on an Iranian military ship that was gathering intelligence on cargo ships in the Red Sea and Gulf of Aden. The operation was designed to prevent the Iranian ship from sharing intelligence with Houthi rebels in Yemen, who have been shooting missiles and drones at cargo ships in the Red Sea. According to several international independent journalists, namely from The Guardian, New York Times, The Walrus, Le Monde, CNN or France 24, amongst many others, Israel is using Artificial Intelligence as a “Weapon of War”. And according to with The Jerusalem Post, an IDF Intelligence Corps senior officer said, “For the first time, artificial intelligence was a key component and power multiplier in fighting the enemy”. This is of great concern, when a machine has the power to decide on targets, where there are civilians.

Meanwhile, it is possible to see to a direct dispute by Israel and Iran, in cyberspace, below the threshold level of war, trying to disrupt societal systems in both countries, with Hacktivism on the rise supporting the two sides of the conflict.

5. To conclude Ukraine and Gaza

Cyberspace is part of two conflicts with different approaches, due to the different capabilities of its actors. In Ukraine the belligerent parts are not following the commitment to the United Nations' norms of responsible state behaviour in cyberspace. The US is a global actor, taking part in the two conflicts. Hacktivism has been growing, aiding both sides in the two conflicts. Artificial Intelligence is also part of them, with different approaches, one being part of the market looking for profits with “the genie’s out of the bottle”, and the other using it for killing purposes.