論　文

The Role of ICT Multinational Companies In Ukraine's Cyber Defence Capability Build-up in 2022-2023

Maksym YAROSHENKO

I. Introduction

Confrontation in cyberspace is intensifying, and companies, people, international organisations, and countries are getting 'sorted', forcing them to choose sides in the conflict between revisionist states and Western democracies(Moss, 2024). Cyberspace is considered a newly emerged, first-ever man-created domain. However, who is responsible for protecting it is a debated issue (Carr, 2016). Generally, it is conceived that the state should be the main actor in protecting infrastructure involving networks and critical infrastructure (CI) within its geographical boundary as a national security issue.

On the other hand, many scholars have started to argue the role of the private actor as one of the key cybersecurity stakeholders (Carr, 2016; Chen, 2020; Christensen & Petersen, 2017). In this context, so-called private-public partnerships (PPPs) have drawn scholars' attention as one of the most significant and prevalent frameworks in which national security is questioned and secured. The ongoing war in Ukraine has manifested both physical (kinetic) and cyber warfare considered. It is essential to pay attention to the case of Ukraine, namely, what cyber defence capability Ukraine attained before the outbreak of the War. This is because Russia's cyber attacks had much less than initially expected effect (Willett, 2022).

Furthermore, from 2014 to 2022, the USA state and other Western countries assisted in strengthening Ukraine's cyber defence capability. However, after the full-scale invasion in 2022, the situation changed, and the private sector got involved and took a clear one side in the war, initially with ad hoc solutions that later were institutionalised and evolved into goal-oriented PPPs (Yaroshenko, 2024). Therefore, the period of 2022-2023 and the case of Ukraine was selected

for this study.

Some scholars have already argued that the remarkable thing is that US multinational enterprises (MNEs) provided much-needed and crucial support to strengthen Ukraine's cyber defence before and during the invasion of the Russian Federation (the RF) in 2022 (Lilly et al., 2023). Beecroft (2022) also interestingly noted that US companies took the initiative to support Ukraine under the patronage of the USA itself despite the fact that the US appeared not to have many benefits initially.

This research addresses the question: what cooperation did Ukraine and the US MNEs initially engage in, and how did their collaborations evolve towards a more goal-oriented partnership if there had been a goal between the two states? By doing so, this research sheds light on the involvement of IT MNEs in the interstate conflict in the cyberspace domain. Exploring this helps to understand the role of the private sector during times of steadily increasing geopolitical tensions and hostility.

Definitions and Methodology

Cybersecurity is defined as preserving the confidentiality, availability, and integrity of information in cyberspace. Cyber defence capability includes prevention, detection, responding, recovering, and learning from incidents and breaches (RAND, 2016).

In the USA, critical infrastructure (CI) is defined by the Cybersecurity and Infrastructure Security Agency (CISA) as 'those assets, systems, and networks that provide functions necessary for our way of life' with 16 sectors critical infrastructure sectors of the economy. However, as was mentioned during the opening keynote panel discussion at Black Hat USA, 2024, by CISA Director Jen Easterly, sectors and enterprises can be changed upon new challenges. It was illustrated by including the national election IT systems in the list after the RF attempted to influence it in 2016. In the UK, critical national infrastructure (CNI) is defined by the National Cybersecurity Center (NCSC) as 'national assets that are essential for the functioning of society, such as those associated with energy supply, water supply, transportation, health and telecommunications.

The definition of PPPs in states' white papers depends on the reliance of the states, their economies, and societies on information communication technologies (ICT). Regarding the definitions of PPP, Ukraine lacks a clear definition, and it is

only briefly mentioned in the national Cybersecurity Strategy (President of Ukraine, 2021). The Cabinet of Ministers of Ukraine is responsible for deciding criteria for what critical infrastructure is and thus assigning which companies belong to CI. However, ambiguity and the possibility of misuse seem to have led to confusion about what critical infrastructure means. For instance, companies can lobby to be included in the list of CI objects, particularly during martial law, because it gives them preferences, including the ability to reserve their employees from being drafted into the armed forces. This research has applied the definition proposed by the European Union Agency for Cybersecurity (ENISA): 'Public-private partnership (PPP) is a long–term agreement/ cooperation/collaboration between two or more public and private sectors that has developed over time in many areas' (ENISA, 2017). After the key definitions are given, the research methodology is presented below.

This multidisciplinary research employs a deductive-qualitative approach. Primary sources such as the USA and Ukraine cybersecurity strategies white papers, related presidential orders, laws and decrees were scrutinised. Primary data is supplemented with findings from secondary sources such as academic articles, media, and reports from multinational IT and cybersecurity companies. Online attendance at Black Hat Asia 2024 and Black Hat USA 2024 contributed significantly to studying the condition of the cybersecurity ecosystems in Asia and North America, helped to supplement findings, and sharpened knowledge about the current geopolitical tensions.

The author regarded fieldwork as an essential tool as this study focuses on contemporary issues. From May to July 2024, the author interviewed cybersecurity experts, IT engineers and entrepreneurs, policymakers, and representatives from business, law researchers and academia. Interviews took place online within the professional network while preparing the foundation for the research. Follow-up interviews were conducted. A substantial amount of data was obtained during research exchanges, follow-up talks after the presentations and in-depth semi-structured interviews at CyberSec Forum and Expo 2024, Krakow, Poland and ECCWS 2024, Jyväskylä, Finland. The author conducted in-person, in-depth, semi-structured interviews with cybersecurity researchers, academia, and business representatives in the EU.

II. What is a Private-Public Partnership?

As discussed above, there is no generally accepted single definition of the PPP, and this fact is clearly mentioned by prominent researchers. Scholars instead are focused on the functions and nature of the partnerships, hence producing categorising frameworks that serve as a theoretical argumentation. The discourse is built around characterising the term, discussing the difficulties PPPs encounter to fulfil a common goal and proposing solutions. The focal points are responsibility and accountability for all sides involved. It is important to note that the State forfeits its basic function as a security guarantor. A knotty dilemma emerges within the PPPs: how to strike a balance between private economic interests and national security. Loyalty, trust, and patriotic motivation are vital for achieving security goals through the PPP scheme. (Carr, 2016; Chen, 2020; Christensen & Petersen, 2017).

Types of PPPs

ENISA categorises PPPs according to four models presented in Figure 1. They differ by the degree of involvement of participating parties and the level of commitment. A goal-oriented PPP fits the case of Ukraine, and this study focuses on how collaboration in Ukraine evolved. The common goal among all stakeholders, namely, the USA, the MNEs, and Ukraine's military, public and private sectors, is to secure Ukraine's networks, particularly the government and critical infrastructure. This goal is shared among all the stakeholders (Lilly et al., 2023)

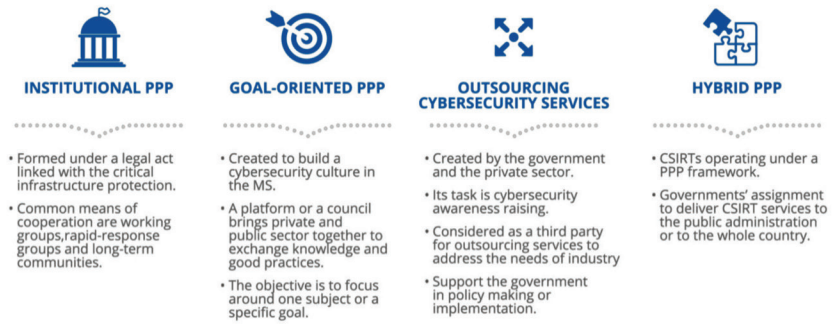

Figure 1, Partnership models

[Source: ENISA, 2017]

ENISA framework is aggregated and doesn't fully cover which factors determine the type of the PPP. Therefore, partnership models are supplemented with Table 1, which illustrates critical factors and their presence in different work methods within PPP. Furthermore, Dr Chen (2020) wisely points out the importance of trust in his writings. As seen from Table 1, trust is not mandatory for situational cooperation. However, for the sake of efficiency and to succeed in complex tasks, collaboration and integration are vital.

Table 1 Differences in partnership methods

Factors	Cooperation	Collaboration	Integration
Trust	May or may not have	May have	Have
Org structure	Horizontal	Horizontal	Hierarchical
Leadership C2	Not designated	May be designated	Designated
Responsibility	Not assigned	May be assigned	Assigned
Liability	Not known	May be known	Known
Relationship	Very loose	Loose	Tight
Communication	Horizontal	Horizontal	Hierarchical
Checks-and-balances	May have	Have	Not have
Budget & Resources	Not allocated	May be allocated	Allocated
Approach Taken	Bottom-up	Bottom-up	Top-down
Common process	May or may not have	May have	Have
Dedicated team	May or may not have	Have	Have
Common goal	May or may not have	May have	Have
Shared strategy	May or may not have	May have	Have
Dedicated Tools	May or may not have	May have	Have

Source: [J. Chen, 2020, p.21]

The benefits of PPPs for both private and public sectors outweigh the risks. Considering the abovementioned hardships, partly inherited from PPPs in other sectors of the economies, three modes of cooperation are introduced. Cooperation, collaboration, integration, and top-down and bottom-up management approaches. The most suitable and appropriate approach to creating a PPP depends on the type of goal the stakeholders of the PPP aim to achieve, the cultural differences of the operational territory, and available resources (Chen, 2020). Cooperation assumes the least amount of commitment and involvement of parties, and integration brings cybersecurity personnel from the MNE to the receiving side, which takes place in the US.

Motivation, willingness to be on the right side of the conflict, and the shutdown of most Western businesses in the RF contributed to the readiness of the US-based MNEs to collaborate and assist Ukraine in providing hardware, software, knowledge, and training. Ukraine's case shall be studied for the successful implementation of PPPs in the future, regardless of the geography. Existing theoretical frameworks and relations between different factors in Table 1 help policymakers select an appropriate scheme for PPP to pursue and promote via national strategies and policies.

Most of the research in the field of this study is done in the US. Furthermore, the US is a significant stakeholder in developing Ukraine's cyber defence. Thus, to understand the nature of the problem, it is vital to discuss how the PPPs in cybersecurity developed in the US during the last 30 years. The theoretical discussion was partly highlighted earlier in this article. The subsection below presents the development of relations between policymakers and the private sector.

The Development of PPPs for Cybersecurity in the US

Policymakers in Western democracies contemplate academia, businesses, and civil society when incorporating PPPs into the country's cybersecurity strategies. This trend has been steady throughout modern political history from the 1990s to the present. An illustrative example is the USA and the evolution of their strategy and policies. This policy started with the B. Clinton administration's emphasis on the importance of the US technological sector and the necessity of its support after the end of the Cold War (Clinton, 1998). Presidential Decision 63 on national cyber policy was published in 1998. Shortly in 1999, J. E Stiglitz and S. J. Wallstein published an influential article. Pundits stress the importance of public-private technology partnerships in R&D efforts (Stiglitz & Wallstein, 1999). Several persistent hurdles emerged due to the nature of the incentives that led politicians, program managers, and firms and the ability to achieve a shared goal. (Stiglitz & Wallstein, 1999, p. 71).

The next milestone was under the B. Obama administration in 2009. Threats to national digital and critical infrastructure were recognised. The White House incorporated PPPs as vital and effective tools in the Cybersecurity Review, which stressed the importance of PPPs in critical infrastructure cyber defence. Understanding the prominence of cooperation with the private sector persisted

and intensified in every cybersecurity strategy document during the last 25 years (Healey, 2023).

The latest Cybersecurity Strategy published by the G. Biden administration in 2023 highlighted the importance of PPP, a development trend during the last 30 years. PPPs were designated pivotal roles to defend critical infrastructure under the collaboration framework. Indirectly, PPPs for cybersecurity are defined as 'We aim to operationalise an enduring and effective model of collaborative defence that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem' (White House, 2023). The successful case of PPPs and collaboration to defend Ukraine's networks was mentioned in Pillar One: Defend Critical Infrastructure. (White House, 2023). In May 2024, the Department of State published another white paper titled United States International Cyberspace & Digital Policy Strategy. The RSA cybersecurity conference in San Francisco was chosen as the place to announce it. The document stresses the importance of collective measures and collaboration to secure and support a resilient multistakeholder Internet. The long-anticipated and much-needed concept of digital solidarity as a counter to digital sovereignty (Roguski, 2023) is at the heart of the white paper (US Department of State, 2024). A. Blinken, Secretary of State, pinpointed the importance of the experience the public and private sectors earned during their collaboration to help Ukraine.

As seen from white papers and strategy development, the role of the private sector in the nation's cyber defence is increasing following the ever-increasing adoption of ICT. However, until the collective efforts to defend Ukraine, there was no practical case of effective collaboration. The next section of this article delves into the assistance provided to Ukraine. It categorises and characterises the help from donor companies. In this context, discussing the blurring line between civil and military sectors in cyberspace is necessary.

III. Private Sector Involvement in Building up Cyber Defence Capabilities in Ukraine

Cyberspace, Challenges to Separate Civil and Military Domains

This research is focused on assistance provided to the civil sector. The reasons are the emphasis of the author's interest in critical infrastructure

protection, public and private networks and services defence. Military support is highly classified, and respondents avoided providing in-depth answers during the interviews as per their agreement with recipients in Ukraine. For this reason, the author conducted another interview with policymakers and business executives at the CyberSec Expo and Forum to investigate assistance provided to the civil sector. However, during interviews, it became evident that the complete separation of civil and military domains is practically difficult because of several complexities illustrated via the case studies below.

For instance, but not limited to, satellite Internet terminals increasingly blur the line between civil and military domains. Italian Navy Commander (OF-4) pointed out during a panel discussion at the CyberSec Forum 2024 in Poland the convergence between military and civil domains in cyberspace (Giovannelli, 2024). Further complexity in the differentiation between civil and military domains is based on concrete examples from Ukraine. This became evident as a part of this research during interviews with IT entrepreneurs, Western MNEs employees, policymakers, and academia. Regarding how to protect cyberspace, it is significant to understand how critical infrastructure can be cyber-challenged by an adversary state like the RF.

In the modern, globalised and interconnected world, enterprises in different parts of the planet often use similar IT systems and business solutions. Ukrainian courier services, banks, CCTV operators, and telecom companies became targets of cyberattacks. Intruders aimed to obtain the personal information of the citizens and access to real-time videos to gather intelligence about the troops' movement and the airstrikes' results. Interviewees mentioned cases discussed below to showcase the most recent experience from Ukraine that shall be studied and applied by other countries as it relates to universal services available in different jurisdictions.

One example is the case of Nova Poshta, Ukraine's private post service. It is a successful company, but seeing the courier as a part of critical infrastructure can be difficult. At times of war and alongside chronically unsatisfactory services provided by the state-owned Post of Ukraine company, Nova Poshta often delivers to the areas affected by war, including the front line. Recipients' locations, names, and other private data are at risk of being compromised. This brings direct danger to Ukraine's servicemen and hence affects national security (Interview, business executive, name not specified to provide privacy).

Another example is, nationalised in 2016, the Joint-Stock Company Commercial Bank PrivatBank. It is responsible for salaries and compensations to the armed forces. Lack of critical thinking and cyber hygiene leads to the fact that every soldier receives his salary with the name of the recipients and the code number of a military unit in the transaction's title. Moreover, the monthly payment amount directly indicates whether the soldier is on the front line. Compensations for injuries and fatalities can be identified. Compromise of such information directly threatens national security and can provide an adversary with valuable intelligence information (Interviews, business executives, names not specified to provide privacy).

Advanced network intrusions and zero-day exploits can often go undetected for a long time. This was evident with the compromise of Ukraine's telecom carriers. A far less known example is Ukraine's road control cameras network and its switch-off during the first days of the invasion in 2022. The government then claimed it was a deliberate move to ensure the enemy could not access it.

However, this research concluded that, as a matter of fact, the adversary took down the network and compromised it before the conflict. The duration of the time the enemy had access to the country's traffic cameras and could track the movement of armed forces remained unknown. This undoubtedly showcases the importance of the holistic approach to cybersecurity and the danger of underestimating a country's IT ecosystem and its members.

Cyber defence operations (CDO) in Ukraine are mainly done under the Intelligence Agency of Ukraine (SBU) responsibility. Hence, there were several obstacles to obtaining information about civilian support, too. SBU asks vendors not to disclose conditions of cooperation. However, this is not particularly wise because the cybersecurity strategies of the NATO states and Ukraine are based on transparency. Revealing the knowledge can help to learn behind successful cases and ease the ability to replicate the experience. Ukraine and the agencies responsible for cybersecurity need to improve their communications and share non-sensitive data with researchers and the community to foster discussion and improve trust. By doing this, Ukraine can improve its procedures and be accountable for the assistance provided.

Information about struggles, such as the case with satellite Internet access Stralink terminals, can contribute to understanding how to overcome difficulties. The SpaceX company provided terminals as the founder, E. Musk, made the

personal decision. However, as the conflict was ongoing at some point, Musk changed his decision and requested payment for the services. Furthermore, blocking access to it at the front lines of the conflict. He reconsidered risks and benefits through the prism of a longer-than-anticipated duration of the war (PCMag, 2024).

The US and other governments intervened in cooperation between Space X and Ukraine, and access was resumed. Terminals have been provided until now and deliver crucial help for drone operators. It is worth noting that despite the sanctions, the RF obtained and currently uses thousands of terminals. Terminals were procured through crowdfunding campaigns and imported from third countries. Ukrainian front-line soldiers point to the decreased speed of the Internet connection, attributing it to the increased number of devices from both sides of the battlefront line (Microsoft, 2022).

The above analysis indicated several new, unanticipated hurdles that emerged during wartime. However, although the numerous assistance measures provided by the US to Ukraine pose security risks for businesses, Western MNEs continue their efforts to help Ukraine. The following subsection will discuss how capability was enhanced.

Defending Ukraine's Cyberspace and Cyber Defence Capability Build-up

As illustrated in the previous section, donors faced many novel difficulties. To address them and increase the efficiency of assistance, particularly during a war in a time-sensitive environment, all the stakeholders agreed to institutionalise the approach. As mentioned, Ukraine started to receive unprecedented and comprehensive aid. Professor Chen, during our research exchange in Jyväskylä, Finland, on the grounds of the European Conference on Cyber Warfare and Security (ECCWS) 2024, knowledgeably pointed to the crucial condition. Successful PPP is only possible when all the parties involved benefit, which is the difficulty that obstructed the collaboration until recently. The paper from proceedings from the International Conference on Cyber Conflict (CyCon), Tallinn 2023, meticulously summarises the assistance provided to Ukraine through the different organisations.

Table 2 Disclosed assistance provided for Ukraine since February 2022

Company	IT Category	IT Category
Amazon	hardware, software, cyber services	Snowball devices, AWS cloud, software, educational devices to help children learn
Atlas VPN	software	VPN subscription
Avast	software	antivirus license
Bitdefender	cyber services	technical consulting, threat intelligence, cybersecurity technology
Boldare	software	app to find accommodation and transportation
Cisco	cyber services	threat intelligence, threat hunting, monitoring
Cloudflare	software	anti-DDoS tools
ESET	cyber services	threat intelligence, malware detection, remediation
Google	software, cyber services	technical infrastructure, digital skills, funding, training
Mandiant	cyber services	threat intelligence, malware detection, mitigation, incident response, compromise assessments
Microsoft	software, cyber services	data centers, cloud migration, storage, threat intelligence, malware detection, vulnerability discovery, patching
Nokia	hardware, software	software, telecommunications infrastructure
Outpost24	software, cyber services	vulnerability scans, threat intelligence
Recorded Future	software, cyber services	cyber threat intelligence, critical infrastructure protection
Sentinel One	software	endpoint protection
Sophos	software	endpoint protection, network security
Starlink	hardware, cyber services	satellite communication
Vectra AI	software	monitoring tools, incident response tools

Source: [Lilly, B., Rattray, G., Geers, K., & Koch, R., 2023]

The analysis of open source information, research exchanges, and interviews was made to categorise the assistance via facilitating organisations. Greg Rattray, a well-known and respected person in the American cybersecurity

community, organised the Cyber Defence Assistance Collaborative for Ukraine (CDAC). Ukraine's needs were well communicated, heard and financially supported. MNEs had the motivation, trust, and all the necessary financial and political conditions to contribute. Cyber defence assistance (CDA) was well coordinated through CDAC. This allowed it to break the ice and establish a collaboration that evolved into PPPs to deliver cyber defence assistance for Ukraine.

In the report published by Aspen Institute in 2023, authors differentiate between cyber defence capabilities build-up and cyber defence assistance, defining it as 'cyber defence assistance (CDA), which refers to cyber support activities provided to friendly or allied nation-states under threat of or actual attack from a hostile nation-state' (Rattray et al., 2023). The goal orientation of the CDA is in line with the PPP partnership models discussed earlier (ENISA, 2017). Furthermore, it does not contradict the overall development of the theoretical background by scholars and policymakers highlighted in section II.

As a result, prominent vendors Avast, Cyber Threat Alliance, Looking Glass, Mandiant (Google), Microsoft, Recorded Future, Sentinel One, Splunk, Symantec/Broadcom, Next Peak, and Threat Quotient joined the initiative. Certain vendors choose to keep their contributions private, so the full impact and all contributions cannot be researched yet. Assistance was provided to secure networks, hunt for and expel malicious cyber intruders, improve attack surface monitoring, and provide cyber threat intelligence (CTI) to protect critical infrastructure.

In 2022, Ukraine received copious amounts of data from different vendors. Data was often duplicated, causing difficulties in understanding and utilising it. It is common sense that the private sector is the most skilful actor in innovation. The CDAC initiative was started by private sector representatives, who brought a novel solution to organising the data flow so Ukrainian partners from different institutions could utilise it efficiently and promptly. A centralised CTI data platform was built, and data was ingested, deduplicated, normalised, enriched, and finally distributed to different entities. Vendors developed a data-sharing capability via classified networks (air-gapped data) (CDAC, 2024).

Certain assistance was institutionalised and administrated via the Tallinn Mechanism established in 2023. In an interview, the cyber attaché responsible for the Estonian office in Kyiv mentioned that the efforts are underway but are

still in the organisational stage (Petrone, 2024). There is still a lack of data, but the long-term goal is political and is to bring the Ukraine legislative environment per the EU standards. However, the total assistance is estimated to be tens of millions of USD. That can be because certain companies, originally ad hoc and later directly supported by their respective governments' assistance, were later formalised and transferred into the newly established mechanism.

USAID's focus in Ukraine before the war was building an independent and resilient cybersecurity ecosystem. Firstly, the organisation helped to address critical governance issues via IT solutions. Later, when cyberattacks from the RF intensified, they invested efforts and funds to help Ukraine develop its own cybersecurity services vendors and facilitate education and training. The organisation has an office in Kyiv and is developing educational capabilities, civil society, and cooperation between Ukraine and international governmental institutions. One of the examples worth noting is the launch of the successful partnership between the State Service for Special Communication and Information Protection and CISA (USAID, 2023). Starting in 2014, their efforts proved successful as Ukraine's cyber defence capability improved. Ukraine surprised the world by being able to repel and be resilient during initial attacks before the invasion.

However, with the outbreak of the invasion in 2022, a more proactive stance was needed as the amounts and complexity of cyberattacks launched by the RF and affiliated actors were unprecedented. USAID led by example and funded Starlink terminals for Ukraine. Furthermore, it cooperated with Cisco to provide network equipment and training. As the assistance started to mature and private companies took the flag, USAID shifted its focus back to supporting educational and research activities. USAID supports cyber education by providing free training and courses in person and online, opening laboratories and providing necessary equipment to universities (KPI, 2024).

Ukraine's Cyber Defence and Tackling Real-time Battlefield Threats

As wartime often requires rapid solutions, let's discuss cases not attributed to the particular initiative. However, they are significant in their scale, complexity, and impact. Crowdstrike provides military and government institutions access to its cutting-edge endpoint protection platform. Before the war, this was out of reach as the government could not afford the high related

costs. The company has not yet disclosed the funding sources and how the collaboration is structured. Amazon provided Snowball devices – cutting-edge data transfer hardware technology and granted access to its AWS cloud services. Ukraine moved massive amounts of governmental data outside the country and out of reach of the adversary (Lilly et al., 2023). Space X's assistance with the Starlink terminal was discussed earlier. Ukraine received over 20000 terminals directly from the company during the first months of the invasion, aid valued as high as 80 million USD (Marquardt, 2022).

Since the early days of the invasion, Google has contributed to securing Ukraine's cyberspace. In early 2022, the Ukrainian government received 50,000 Google Workspace licences with a one-year free licence to enable public institutions to continue to perform their functions despite a highly disruptive and hostile environment (Google, 2022). During the first year of the invasion, protection against DDoS attacks was provided, and eventually, Google joined collective efforts under the CDAC (Google, 2023). The Mandiant part of Google is doing complex, essential work in analysing and providing threat protection against advanced persistent threat (APT) actors associated with GRU, the RF intelligence service (Mandiant, 2024). Initial assistance was financed by CSSF UK-Ukraine Cyber Programme, which later merged into TM (UK Government, 2023).

Google (Alphabet) and its cybersecurity arm, Mandiant, contributed significantly to Ukraine's cyber defence. Aside from the assistance discussed above, needed measures were organised directly between the executives of Ukraine's state-owned oil and gas company Naftogaz and Mandiant. In 2022, R. Bushar, CTO of Mandiant, made a voluntary call to the executives of Naftogaz, offering assistance in checking company networks for threat actors. The extensive Mandiant security team promptly inspected the company's perimeter (sweeping the networks), which is usually a complex and time-consuming process. No massive intrusions or threats were found, existing ones were eliminated, and the company networks were secured and fortified.

Nevertheless, malicious codes and wipers were re-emerging. This was attributed to the insider threat, which stems from the fact that the RF troops advanced through Ukrainian territory, occupying the company's facilities and offices. Offense teams from the RF gained access to computers and networks. The Naftogaz company promptly instructed its employees to cut off the

networks in case of the invading army's proximity. Mandiant was helping cut off the company premises' networks in the occupied territories. In the face of such an unexpected threat during the war, cooperation ensured the security of Naftogaz's IT infrastructure, which is critical for the whole country. For the Mandiant, it provided valuable battlefield experience (The Record, 2022). This case portrays novel, evolving threats during the war and how both parties of the PPP can benefit from the cooperation while securing the nation's CI during real-time military actions.

Microsoft assisted Ukraine in transferring many government operations and data into the cloud and data centres. The project involved 20 ministries, over 100 agencies, and state-owned companies. The total cost of the assistance provided is 107 million USD (Microsoft, 2022). The company actively helps Ukraine with cyber threat intelligence sharing and commits significant efforts to counter the activities of APT groups associated with the RF's intelligence agencies (Microsoft Digital Defence Reports). To incorporate the assistance provided by Microsoft and earlier discussed data transfers from Ukraine's servers to safe locations abroad using Amazon Snowball devices, the national law governing all public data to be stored inside the country was changed at the initiative of Ukraine's Digital Transformation Ministry in February 2022.

Additionally, Microsoft actively participates in information warfare; the Russian Propaganda Index is one distinctive tool. The corporation actively lobbies for Ukraine among US political and business leaders (Watts, 2024). In addition to significant personal commitments, Microsoft has joined numerous partnerships. As a global political player, Microsoft is at the forefront and has initiated collective measures to secure the multistakeholder Internet, such as the Cybersecurity Tech Accord (Yaroshenko, 2024).

Cybersecurity Tech Accord is an initiative that started in 2017 and was a response to the increasing levels of cyberattacks, including Not Petya, attributed to the RF intelligence services-affiliated Advanced Persist Threat (APT) group. Its impact went beyond Ukraine and was condemned by the White House (Trump, 2018). Cybersecurity Tech Accord was initially proposed by Microsoft and had 34 original signees. Currently, over 150 tech companies have joined the shared effort with four principals (Cyber Tech Accord website, 2024):

- Protect all of our users and customers everywhere;
- Oppose cyberattacks on innocent citizens and enterprises from anywhere;

- Empower users, customers and developers to strengthen cybersecurity protection;
- Partner with each other and with like-minded groups to enhance cybersecurity.

Challenges in separating civil and military domains in cyberspace pose consequent risks for MNEs being involved in military confrontations between nations and their allies. Despite this, global ICT companies not only provided initial empathetic assistance with side situational benefits, such as reputational gains and knowledge, but also proceeded to mid-term and long-term goal-oriented partnerships. In the Ukrainian case, stakeholders found agreement and moved towards the collaboration that state development agencies and private sector initiatives institutionalise.

As the definition mentions, cyber defence capability includes prevention, detection, response, recovery, and learning from incidents and breaches. Ukraine received the necessary hardware, software, and cybersecurity services to establish adequate capability for defending its networks. The capability was provided by Western MNEs, patronised, and protected by the ally state, the USA. Case studies in this section explained what was done, how it was accomplished, and what hurdles were encountered. This allows us to address the main research question and provide the result of the hypothesis testing in the conclusion below.

IV. Conclusion

Over the last three decades, policymakers, academia, and civil society in the USA and NATO member states have reached a consensus about the cornerstone role of ICT in national security. As ICTs became more complex and implemented more widely, each government started to develop cybersecurity policies as an urgent task.

Ukraine's cybersecurity capability developed significantly with external assistance during 2014-2023. There is still a lack of clear legislation today in Ukraine to fully implement what is stated in white papers and frameworks, compared with the USA and NATO members of the EU. However, it should be noted that no successful blueprint existed until recent years for collective measures to defend Ukraine's cyberspace. Ukraine has recognised that there is

an urgent need to develop cyber defence capability in the format of white papers that the US published earlier. As discussed in the "The Development of PPPs for Cybersecurity in the US" subsection, the most recent white papers published in the US stress the need to study Ukraine's case further and replicate it in other jurisdictions, including the securitisation of US domestic networks. Thus, the US government started to initiate its support plan for Ukraine as early as 2014.

Cybersecurity is a collective and expensive sport, and a holistic approach is vital. As the industry traditionally produces innovation and the private sector dominates the rapid development of cybersecurity technologies, stakeholders have shifted from the government or state to more diverse actors. As a result, as analysed earlier, PPP has become a significant framework for building up cyber defence capability. It is generally conceived that a common goal, trust, responsibility, and accountability are the foundations of a successful PPP.

Cybersecurity ecosystems and threat landscapes have developed rapidly and asymmetrically in different world regions. Only robust collaboration with international ICT MNEs can provide solid solutions to secure networks in these circumstances. Interdisciplinarity and horizontal cooperation between policymakers, industry, academia, and civil society have become necessary to adequately address modern challenges.

In Ukraine, the initial ad hoc approach was institutionalised. The private sector's initiative, CDAC, developed a centralised cyber threat intelligence data-sharing platform. USAID took the initiative even though it was outside the scope of its core activities.

Dual-purpose technologies and blurring lines between civil and military sectors are emerging challenges. Securing each component is vital for the systems' overall stability as the world becomes further connected and digital ecosystems expand. This article's case studies illustrate challenges during the modern military confrontation:

- Private information security;
- Targeting civil infrastructure and private companies for espionage purposes;
- The importance of personal connections to navigate the fog of war;
- Reliance on private sector solutions for connectivity (Starlink) and cyber threat intelligence (CTI) gathering.

The current case with Ukraine signified that the USA mobilised the private

sector to perform security functions for the other sovereign country. Due to the modality of PPPs that the US government utilised, the US assistance has not appeared to be interventional. On the other hand, it seemed natural that the US played a vital role in strengthening Ukraine's cyber defence capability as it owns a global digital defence role without much financial and operational burden. Thus, this research demonstrated a paradigm shift in the nation's cyber defence, where the private sector plays a pivotal role. Security is conventionally the state's responsibility, but appropriated usage of the PPPs scheme is a powerful tool for the benefit of both the public and private sectors.

References

Beecroft, N. (2022). Evaluating the international support to Ukrainian cyber defense. Carnegie Endowment for International Peace. [https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en (Accessed August 22, 2024) (Accessed August 22, 2024)

Blinken, A. (2024). Technology and the Transformation of U.S. Foreign Policy. RSA Conference. San Francisco. Opening Keynote.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, vol. 92:1, 43-62.

Chen, J. Q. (2020). A Framework of Partnership. The Cyber Defense Review, vol. 5:1, 15-28. Army Cyber Institute.

Christensen, K. K., & Petersen, K. L. (2017). Public-private partnerships on cyber security: a practice of loyalty. International Affairs, vol. 93:6, 1435-1452

CDAC. (2024). Cyber Defense Assistance Collaborative (CDAC) Case Study: Threat Intelligence Sharing.

Clinton. (1998). White paper: The Clinton administration's policy on critical infrastructure. National Criminal Justice Reference Service. [https://www.ojp.gov/ncjrs/virtual-library/abstracts/white-paper-clinton-administrations-policy-critical-infrastructure] (Accessed September 3, 2024)

CRDF Global. (2022). CRDF Global becomes platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine, receives grant from Craig Newmark Philanthropies. [https://www.crdfglobal.org/news/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-receives-grant-from-craig-newmark-philanthropies/] (Accessed August 22, 2024)

CRDF Global. (2023). Cyber Defense Assistance Collaborative sends delegation to annual CyCon conference in Tallinn to develop cyber defense assistance for Ukraine. [https://crdfglobal-cdac.org/cyber-defense-assistance-collaborative-sends-delegation-to-annual-cycon-conference-in-tallinn-to-develop-cyber-defense-assistance-for-ukraine/] (Accessed August 22, 2024)

CRDF Global. Who we are. CRDF Global. [https://crdfglobal-cdac.org/who-we-are/] (accessed August 22, 2024)

CyberTech Accord. Signatories. (2024) [https://cybertechaccord.org/signatories/] (accessed August 22, 2024)

CyberSec Expo & Forum. (2024, January 22). Establishment of the Tallinn Mechanism: Polish

support for Ukraine's cybersecurity. CyberSec Expo & Forum. [https://cybersecforum.eu/2024/01/22/establishment-of-the-tallinn-mechanism-polish-support-for-ukraines-cybersecurity/] (accessed August 22, 2024)

ENISA. (2017). Public Private Partnerships (PPPs) Cooperative models.

Giles, K. (2023). Russian cyber and information warfare in practice. Chatham House. [https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/03-distinctive-features-war] (accessed, June 6, 2024).

Global Affairs Canada. (2023). The Tallinn Mechanism: Enhancing cybersecurity and international collaboration. [https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/tallinn-mechanism-mecanisme-tallinn.aspx?lang=eng] (accessed, August 22, 2024).

Google. (2022). New ways we're supporting Ukraine. [https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine/] (accessed, August 22, 2024).

Google Threat Analysis Group. (2023). Fog of war: How the Ukraine conflict transformed the cyber threat landscape. [https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/] (accessed, August 22, 2024).

Healey, J. (2023). Twenty-Five Years of White House Cyber Policies. Lawfare. [https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies] (accessed, June 6, 2024).

Interfax. (2024, August 28). Microsoft starts rolling disconnection of its cloud products in Russia. Interfax. [https://interfax.com/newsroom/top-stories/102413/] (accessed, July 22, 2024).

KPI. (2024). Title of the web page. Kyiv Polytechnic Institute. [https://kpi.ua/en/2024-08-20] (accessed, August 22, 2024).

Kyiv School of Economics. (2023). Google finally left the Russian market in October, along with 11 other companies [https://kse.ua/about-the-school/news/google-finally-left-the-russian-market-in-october-along-with-11-other-companies-kse-research/] (accessed, August 22, 2024).

Liebetrau, T., & Monsees, L. (2023). Assembling Publics: Microsoft, Cybersecurity, and Public - Private Relations. Politics and Governance, vol. 11:3, 157–167.

Lilly, B., Rattray, G., Geers, K., & Koch, R. (2023). Business@War: The IT companies helping to defend Ukraine. In Proceedings of the 2023 15th International Conference on Cyber Conflict.

Mandiant. (2024,). GRU's disruptive playbook: How Russia's military intelligence agency operates online. [https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook] (accessed August 22, 2024)

Marquardt, A. (2022). Elon Musk's SpaceX threatens to cut off Starlink to Ukraine. CNN. [https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html] (accessed August 22, 2024)

Microsoft. (2022). Defending Ukraine: Early lessons from the cyber war 2022. [https://www.microsoft.com/en-us/security/blog/2022/05/24/defending-ukraine-early-lessons-from-the-cyber-war-2022/] (accessed August 22, 2024)

Microsoft. (2024). Update on Microsoft actions following attack by nation-state actor Midnight Blizzard. Microsoft Security Response Center. [https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/] (accessed August 22, 2024)

Ministry of Defense of Ukraine. (2024, May 31). The IT Coalition led by the Ministry of Defense of Ukraine announces new cybersecurity initiatives. [https://www.mil.gov.ua/

en/news/2024/05/31/the-it-coalition-led/] (accessed August 22, 2024)
Moss, J. (2024). Democracy's biggest year: The fight for secure elections around the world. Black Hat USA 2024. Las Vegas, Opening Keynote.
Oliker O., Davis L. E., Crane K., Radin A., Gventer C., Sondergaard S., Quinlivan J. T., Seabrook S. B., Bellasio, Jacopo, Frederick B., Bega A., and Hlavka J. (2016). Security Sector Reform in Ukraine, RAND Corporation.
O'Neill P. H. (2022). Russia hacked an American satellite company one hour before the Ukraine invasion, MIT Technology Review. [https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine- invasion/]] (accessed, February 3, 2024).
Paganini, P. (2023). APT29 is targeting cloud services in espionage campaigns. Security Affairs. [https://securityaffairs.com/159629/apt/apt29-targeting-cloud-services.html] (accessed, May 28, 2024).
PCMag. (2024). Russia Again Threatens to Attack Starlink, Citing US Spy Satellite Risk. [https://www.pcmag.com/news/russia-again-threatens-to-attack-starlink-citing-us-spy-satellite-risk] (accessed, June 6, 2024).
Petrone J. (2024).Interview with Lauri Luht: The Tallinn Mechanism and its impact. e-Estonia. [https://e-estonia.com/interview-with-lauri-luht-tallinn-mechanism/] accessed (accessed August 22, 2024)
President of Ukraine. (2021). The Cybersecurity Strategy of Ukraine.
Rash, W. (2022). CISA Issues 'Shields Up' Warning About Russian Cyber Attacks. Forbes. [https://www.forbes.com/sites/waynerash/2022/02/25/cisa-issues-shields-up-warning-about-russian-cyber-attacks/?sh=7b6b5c093748] (accessed, June 6, 2024).
Rattray, G., Brown, G., & Moore, R. T. (2023, February). The cyber defense assistance imperative: Lessons from Ukraine. Aspen Institute. [https://www.aspeninstitute.org/report/the-cyber-defense-assistance-imperative-lessons-from-ukraine/] (accessed, August 23, 2024).
RBC Ukraine. (2024). Russia confiscates over $100 million from Ukrainian accounts. RBC Ukraine. [https://newsukraine.rbc.ua/news/russia-confiscates-over-100-million-from-1724592475.html] (accessed, August 23, 2024).
Reuters (2022). White House vows response if Russia attacks U.S. satellites. [https://www.reuters.com/world/white-house-vows-response-if-russia-attacks-us-satellites-2022-10-27/] (accessed, August 23, 2024).
Roguski P. (2023). Digital sovereignty - shaping regulatory responses to technological dominance. CodeBlue. Tokyo.
Stiglitz, J. E., & Wallsten, S. J. (1999). Public-Private Technology Partnerships: Promises and Pitfalls. American Behavioral Scientist, 43(1), vol. 52-73. Sage Publications, Inc.
The Record. (2022). Rounding up a cyber posse for Ukraine. [https://therecord.media/exclusive-rounding-up-a-cyber-posse-for-ukraine] (accessed August 22, 2024)
Treverton G. F. and Esfandiary P. (2022). Will the Ukraine War Reshape the Internet?, Center for Strategic and International Studies (CSIS).
Trump, D. J. (2018). Statement by the Press Secretary. The White House.[https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/] (accessed August 22, 2024)
[https://www.president.gov.ua/documents/4472021-40013] (accessed August 22, 2024)
UK Government. (2023, May 23). UK and partners form the Tallinn Mechanism for cyber security. [https://www.gov.uk/government/news/uk-and-partners-form-the-tallinn-mechanism-for-cyber-security] (accessed August 22, 2024)

US Department of State. (2024). United States International Cyberspace & Digital Policy Strategy

USAID. (2022).Ukraine Fact Sheet Cybersecurity [https://www.usaid.gov/sites/default/files/2023-01/Cybersecurity_eng.pdf] (accessed August 22, 2024)

USAID. (2023). USAID announces $60 million to bolster Ukraine's cybersecurity. [https://www.usaid.gov/news-information/press-releases/feb-10-2023-usaid-announces-60-million-bolster-ukraines-cybersecurity] (accessed August 22, 2024)

USAID. (2024). Every Ukrainian now making their contribution to our common victory: One Ukrainian youth learns cybersecurity to fight Russia's war of aggression. [https://www.usaid.gov/ukraine/news/feb-23-2024-every-ukrainian-now-making-their-contribution-our-common-victory-one-ukrainian-youth-learns-cybersecurity-fight-russias-war-aggression] (accessed August 22, 2024)

Yaroshenko M. (2024). Expansion of NATO and Ukraine: Cyber Dimension and Role of Information Technology (IT). Journal for Information, Study and Discussion of Global Resource Management, vol. 10, 20-41.

Watts, J. (2024, March 25). Ukraine's use of Starlink drones in the conflict with Russia. CNN. [https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html] (accessed August 22, 2024)

White House. (2023). Cybersecurity Strategy.

Willett M. (2022). The Cyber Dimension of Russia–Ukraine War, Survival, vol. 64:5, 7-26.

Abstract

The Role of ICT Multinational Companies In Ukraine's Cyber Defence Capability Build-up in 2022-2023

Maksym YAROSHENKO

In conventional international relations studies, the majority of security is traditionally considered the state's responsibility. However, in the case of national cyber defence, private companies are taking a more proactive approach and actively participate in capability build-up despite directly confronting adversary states. Their role is increasing with the development of the Internet and the ever-broader adoption of information communication technology (ICT).

This article examines what assistance Western Multinational Enterprises (MNEs) provided Ukraine in building up cyber defence capability in the initial stage of the full-scale war in Ukraine, that is between 2022-2023. By so doing, this study will illustrate how well-established companies, such as Google (Alphabet), Microsoft, Amazon, and SpaceX, are among those who assisted. On the other hand, private companies were not alone in their involvement in aid to Ukraine. A private-public partnership (PPP) scheme was one of the representative forms of cooperation between private companies and Ukraine. The study attempts to show a trend of increasing involvement of the private sector and its cooperation with the government seen through a case study of Ukraine.

Keywords: Cyber defence, private-public partnership (PPP).

Acknowledgements

This work was supported by JST SPRING, Grant Number JPMJSP2129. The author would like to express his earnest gratitude to those who agreed to contribute and participate in interviews to prepare this paper. Y. Gatupov from iIT Distribution. A. Chernyavskaya, Y. Zhurer and other team members from Ekran Systems Security Software. V. Sokolovskyi from Go Wombat OÜ. Despite busy schedules, many policymakers and scholars were kind enough to find time to answer questions after numerous presentations and panel discussions at

CyberSec Forum and Expo 2024 Krakow and ECCWS 2024 in Jyväskylä, Finland. This paper would lack many findings without contributions from the author's professional circle of cybersecurity researchers from Western MNEs, IT engineers, cybersecurity scholars and corporate sector executives from Ukraine.