POLICY PAPER

EU'S & UKRAINE'S APPROACHES TO DIGITAL DIPLOMACY

IN THE GEOPOLITICS OF TECHNOLOGIES

VIKTORIIA OMELIANENKO

UKRAINIAN PRISM

Contents

Executive summary

"Digital issues are no longer just technical matters. They are the battleground of technology, of values and narratives" stated Josep Borrell in July 2022.

Within the last decade, geopolitics and strategic competition have been affected by technology development. States stand for their digital sovereignty, make innovation and engagement in global digital and technology governance a part of their diplomacy. Moreover, the Russian invasion of Ukraine has shown the importance of Ukraine applying technologies in both defensive and offensive capabilities. AI systems, an army of drones, satellite communications, back-ups of data, the governmental app Diia with digital services, documents, and the opportunity to share data about the enemy troop's location are a few of the examples that have helped Ukraine to prove resilient in the digital domain in the biggest war in Europe Since WW2.

In recent years, the EU has advanced with the number of regulations of technologies based on the democratic and human-centred approach. Such regulations promote the 'Democracy-technology nexus', i.e. the advancement of technologies that safeguard human-rights protection and benefit citizens in different aspects from the economy to the health and education sectors. That is the approach promoted by the global democracies like the EU and the US and on the contrary faced with the 'digital authoritarianism' – the use of digital information technology by authoritarian regimes to survey, repress and manipulate domestic and foreign populations. In this regard, the EU has realised the need to promote its approach to regulation of digital policies based on democratic values at the so-called 'geopolitical battleground'. With the Council Conclusions on digital diplomacy dated July 2022, the EU has defined digital policy as part of its external action.

Considering the increasing role of digital policy in the EU's foreign policy, it is important for Ukraine to take best practices from the EU. Ukraine is an advanced digital country, but it has not paid enough attention to making its digital policy serve its foreign policy priorities. In times of full-scale invasion, the question of increasing its power through technology and building closer cooperation with both international actors and Big Tech Companies has taken on a new dimension in Ukraine's context, but rather in an emergency way. The same comes for the need and efforts of Ukraine to promote its Ukraine's best practices in digital and cyber resilience at the global level.

The goal of the paper is to research how the EU builds its digital-foreign policy nexus and how it increases its influence in global technology governance while promoting its values and interests. For this, the outlook of the EU digital diplomacy initiatives will be taken into consideration, including a detailed analysis of its partnerships in the domain of its digital and cyber policies. The recommendations will be suggested for the EU policymakers specifically on how to enhance EU' digital diplomacy towards further support and engagement with Ukraine and generally the EaP region. But the main objective of this document is to define on the basis of the EU practices how Ukraine's digital and cyber security policies as well as a large number of private-public partnerships with tech companies can serve Ukraine's foreign policy priorities. The recommendations provide ways on how Ukraine should update its approach to digital diplomacy from the principle of 'learning by doing' to a strategic and comprehensive one, especially considering the global evolving context of the geopolitics of technologies and the war setting.

1. Technologies and geopolitics: where is the place for the EU

The application of technologies in warfare and the advancement of technologies in other states made the EU look at its capability and global positioning, especially in view of China's assertiveness in the digital space and former President Trump's protectionist policy. Geopolitically the EU finds itself between 2 states that strategically compete in the domain of technology trying to strengthen their position in international settings and debates on the technologies in all possible ways.

For example, China has demonstrated its ambition to become the leader in the domain of Artificial intelligence by 2030 stating in its 'Next Generation Artificial Intelligence development plan that "AI theories, technologies, and applications should achieve world-leading levels, making China the world's primary AI innovation center". China exports the 'sophisticated surveillance systems' to at least 18 states and helps another 36 states to repress freedom of speech with its training and seminars. Moreover, about 70% of 4G networks in Africa are produced by Huawei which makes countries dependent on the Chinese-supplied infrastructure.

As for the US, leaving the rule-setting to the market has resulted in the creation of a powerful tech sector in the US that is now comprised of big tech companies – GAFAM - Google, Amazon, Facebook (META), Apple, and Microsoft. They significantly effect domestic and international technology governance through lobbying and serve as an instrument of the US soft power. The link between digital technological policy and US foreign policy can also be traced in the Interim US National Security Strategy. The US wants to lead in the establishment of new rules and practices in the advancement of technologies by renewing the US leadership positions in multilateral organizations such as the UN so that it continues to pursue 'universal values, aspirations, and norms' and not the authoritarian agenda. Moreover, the US sets to "shape emerging technology standards to boost our security, economic competitiveness, and values" along with the 'democratic states', where the EU is one of them.

Europe does not have the worldwide digital champions like the US with its Big Tech Companies – GAFAM and China with Baidu, Alibaba, Tencent, and Xiaomi (BATX) and has imported information and communication technologies, being more dependent on the US rather than China. For example, The EU Digital Compass 2030 says that "90% of the EU's data is managed by US companies, less than 4% of the top online platforms are European, European-made microchips represent less than 10 % of the European market". That reveals the need for the EU to manage its own independence and to achieve its goals in the promotion of its voice in global technological governance at the same time.

The concept of the geopolitics of 'new technologies' was mentioned first at the meeting of the Foreign Affairs Council in July 2021. In the conclusions, the EU recognized the technologies as a 'driver of geopolitical and global influence'. Foreign Affairs Council has set up the objective for the EU to link its digital policies with the external global action of the EU. The instrument for this is the EU foreign policy, especially digital diplomacy. The Ministers have claimed publicly the need for the use of the "EU's capacity as a regulatory power to influence global norms and standards in this field and to ensure that the system remains open, human-centered and based on the rule of law".

EUROPE'S APPROACH TO ITS DIGITAL POLICY IS ABOUT ENSURING THE EMPOWERMENT OF BUSINESSES AND SOCIETIES AND BUILDING A RESILIENT AND SECURE ECOSYSTEM OF DIGITAL TECHNOLOGIES WHILE CREATING LEVEL-PLAYING FOR FOREIGN ACTORS IN THE EU MARKET.

The communication of the European Commission "Shaping European Digital Future Europe" states that it wants to be a 'global player' and "the EU should have leverage with its regulatory power, reinforced industrial and technological capabilities, diplomatic strengths and external financial instruments to advance the European approach and shape global interactions". The current 2022 EU strategy on standardization claims the EU's objective to "shape international standards in line with its values and interests but it is in strong competition to do so". Last but not least, 2030 Digital Compass: the European way for the Digital Decade – the central regulation of the EU on digital policies, including technologies enhances the need for building "strong international partnerships that would enhance the global leadership of the EU in the domain".

Another important term regarding the geopolitical dimension of technologies – is "digital sovereignty". It emerged as the result of the concept of strategic autonomy defined by the EUGS. Strategic Compass refers to it the critical technology areas with the purpose of making the Union resilient, mitigating 'strategic dependencies' and reducing value chain vulnerabilities. These come for all technologies such as AI, modern connectivity infrastructure, and semiconductors supply chains as well as it means increasing the cyber resilience and cyber capabilities both at the EU level and the level of Member states.

2. EU digital-foreign policies nexus: approach and instruments

The term digital diplomacy is often used interchangeably with cyber diplomacy, and tech diplomacy and sometimes is even confused with the concepts of Twitter Diplomacy. At the EU level, there are two official terms – digital and cyber diplomacy. They are much broader than the rest of the concepts but should not be used interchangeably. In turn, tech diplomacy is part of the EU approach to digital diplomacy. But it will be used in the document for defining the private partnerships and relations with Big tech companies.

2.1 Digital diplomacy

With the Council conclusions dated July 2022, the EU has defined digital diplomacy as an integral part of its external action. Overall, it is based on promoting universal human rights and fundamental freedoms, the rule of law and democratic principles in the digital space, and advancing a human-centric approach to digital technologies in relevant multilateral fora and other platforms. Crucial for this purpose are partnerships with like-minded partners and cooperation in and with the UN system, the G7, the OSCE, the OECD, the WTO, NATO, the Council of Europe, and other multilateral fora.

At the institutional level, the Conclusions encourage the High Representative and the Commission to engage at the global level in promoting the EU regulations and build constant dialogue internally with the Member States on the exchange of best practices on digital diplomacy. The EU has Vice-President Margrethe Vestager, who is responsible for the strategic direction of the political priority "Europe Fit for the Digital Age". In practical terms, the EEAS with its representations is leading the digital policy outreach and is supported by the expertise of DG CNECT. Some of the experts of DG CNECT are also seconded to the delegations in China, Brazil, and the US. In September 2022 the EU set up an office in San Francisco. It seeks to promote EU standards and technologies, digital policies and regulations and governance models, and to strengthen cooperation with US stakeholders, including by advancing the work of the EU-US Trade and Technology Council.

THE EU APPROACH TOWARD THE DIGITAL-FOREIGN POLICY NEXUS HAS BECOME MORE COORDINATED AND FOCUSED SINCE 2022.

Among specific tasks for the EEAS, the Commission and Member states the Council's Conclusions on digital diplomacy define:

- Promote new and innovative digitalization tools developed by the European Union, such as technologies, standards or data sets developed in EU programs.
- Explore additional initiatives to increase the visibility of the EU globally by learning from best practices of the Member States.
- Ensure complementarity and coherence between the EU's and Member States' internal and external digital policy initiatives and effective action.

- Develop tailored approaches to build coalitions and strengthen cooperation in multilateral fora.
- Make full, systematic, and coordinated use of the network of EU Delegations and Member States' representations to work with third countries, international organizations as well as the multi-stakeholder community, conveying EU positions and strengthening reporting on technology policy issues.
- Strengthen regional digital diplomacy hubs in key EU Delegations
- Develop digital diplomacy training for EU's and Member States' diplomats to improve skills and to establish a common understanding of technology in geopolitics, and make sure that European diplomacy is fit for the digital age.

3 INSTRUMENTS WHICH THE EU APPLIES IN ITS EXTERNAL ACTION WITH REGARD TO DIGITAL TECHNOLOGIES CAN BE DEFINED.

- **The external effect of its regulatory acts**

The EU, unlike China and the US, uses its regulatory power – the well-known 'Brussels effect' to externalize its influence on the global scale and make foreign actors play by the EU rules in its own market. Starting from the effect of the DGPR the EU expects the same global and ground-breaking effect from the Digital Services Act, and Digital Markets Acts. In turn, some of the flies mostly serve the second goal – construction of the rules for the market and support of the domestic capabilities – like the EU Chips Act and proposed EU Cloud Certification Scheme.
When it comes to the EU's Artificial Intelligence Act, it is a milestone in designing the risk-based approach to the regulation of the technology that is widely discussed now at the global scale. Its main objective is to exclude the EU market from the application of unacceptable technologies including the biometric and mass surveillance technologies used in public areas that are against the EU principles of privacy and pose "a clear threat to the safety, livelihoods, and rights of people". But at the same time, the AI Act gives the EU the leverage in shaping global norms and standards of trustworthy AI and serves as the basis of further engagement "with its external partners, including third countries, and at international fora on issues relating to AI."

- **The partnerships of the EU built at the multilateral, bilateral, and regional levels for the engagement in global technology governance.**

At the bilateral level, EU-US Trade and Tech Council is one of the main examples of the realization of EU digital diplomacy in terms of cooperation with a "like-minded partner". However, the engagement of the EU with both the US and China is necessary for the creation of a 'level-playing field' where the companies of both actors will play by the EU rules. But with the US, the EU has much more in common regarding the values and views on the future liberal order. The EU's engagement in the coordination of the AI policy at TTC is the possibility to exercise influence on the US in this regard. Transatlantic cooperation has got a new dimension in the digital field with the TTC establishment in 2021. The Council meets 2 times a year and is divided into 10 working groups led or co-led by relevant departments, services, or agencies, to operationalize the political decisions and coordinate the technical work. The last meeting took place in December 2022 and it discussed among other things digital Infrastructure and connectivity, cooperation on emerging technologies, building resilient semiconductor supply chains, promoting values worldwide and reaching out to partners, stepping up transatlantic work toward sustainable trade, enhancing security through export controls and investment screening, further growing transatlantic trade, nurturing talent for the digital transition. Apart from TTC, the EU is engaged in bilateral cooperation with India on the basis of the Trade and Tech Council launched in 2023, with Japan and South Korea via established Digital partnerships.
At the multilateral level, the example of the EU digital diplomacy – coordination of the EU and its MS on common positions on strategic elections and appointments at the relevant multilateral bodies. The elections in September 2022 of Doreen Bogdan-Martin (US) as the new International Telecommunications Union (ITU) Secretary General, and Tomas Lamanauskas (Lithuania) as the

ITU Deputy Secretary General, both officially supported by the EU, provide an example of successful European coordination to agree on common support for candidates.

At the regional level, the EU's engagement with the Eastern Partnership is one of the examples. The EU welcomes and encourages the European integration processes in the Eastern Partnership, and digital transformation is one of the priorities. Implementation and adoption of the EU regulatory acts in the digital domain also serve the EU digital diplomacy goals – in promoting human-centered democratic technology governance and resilience in EaP states through its regulatory acts and the establishment of partnerships. In this regard, the EU provides constant assistance and is engaged in the EaP digital transformation process.

An example of such engagement and support at the regional level is the EU4Digital Initiative. EU4Digital aims to extend the European Union's Digital Single Market to the EaP partner states, developing the potential of the digital economy and society, in order to bring economic growth, generate more jobs, improve people's lives and help businesses. Through the initiative, the EU supports the reduction of roaming tariffs, the development of high-speed broadband to boost economies and expand e-services, coordinated cyber security and the harmonization of digital frameworks across society, in areas ranging from logistics to health, enhanced skills, and the creation of jobs in the digital industry.

- **Partnerships with the Big Tech companies while preserving its 'digital sovereignty.'**

Tech diplomacy is actually mostly about relations with Big Tech companies. It is set at the level of the Member states without recognition in the official EU documents. Denmark is a more specific example that has linked technologies and digitalization with a foreign policy with the establishment of the Techonomic approach with the purpose to "make sure that democratic governments set the boundaries for the tech industry - and not the other way around". Thus Denmark has the first world Tech Ambassador whose office has a presence in the technological hubs in – Silicon Valley, Beijing as well in Copenhagen and deals with the influence of Big Tech. At the level of the EU, EEAS recognized the need to cooperate with the Big Tech Companies by opening an office in San Francisco. The main focus of the office is the promotion and the dialogue on the DMA and DSA Acts as they directly have an impact on the Big tech companies who have their word in the global digital policy from digital services to the undersea cables deployment and digital infrastructure.
Furthermore, tech diplomacy can be defined in terms of limiting the access to some of private companies to the EU market. The US's dependence on Chinese telecommunication technologies resulted in the ban of Huawei equipment in the US, and the launch of the 'Clear Network' initiative. The US pushed the EU to agree to the ban on the 5G Huawei network in Europe, using the argument of the security of communication between the EU and the US. However, instead of this, Europe has invented its own 5G toolbox that guarantees the security of its networks and sets for the member states the rules on the security standards for companies who want to operate in the market of 5G in Europe that is more within its foreign policy strategy and rooted in its strategic autonomy. The application of Huawei technologies in the Member states also differs. For example, when Germany was going to refuse the use of Huawei equipment in its 5G infrastructure, the Chinese Ambassador made threats of tariffs on the export of German cars. But after 2020 Member states align with the EU 5G security toolbox.

2.2 Cyber diplomacy

EU digital diplomacy is defined to reinforce the EU cyber diplomacy, as the technology-security nexus needs no explanations. Cyber Diplomacy has been on the EU agenda much longer than digital diplomacy – since 2015 with the first Conclusion of the Council of the EU on Cyber Diplomacy that has enforced the irreversible course of the interconnectivity and the threat of the cyber-attacks that comes across the borders. In 2017 the EU launched its Cyber Diplomacy toolbox. From the political perspective, it legitimizes the use of the measures within the Common

Foreign and Security Policy, including, if necessary, restrictive measures toward countering and responding to malicious cyber activities. The EU has committed to the promotion of security and stability in cyberspace through increased international cooperation, and at reducing the risks of misperception, escalation, and conflict that may stem from ICT incidents. The EU framework for restrictive measures against cyber-attacks threatening the EU and its member states was set up in May 2019. In 2022 the framework for restrictive measures against cyber-attacks threatening the EU and its member states was extended for a further three years, until 18 May 2025. Sanctions currently apply to eight individuals and four entities and include an asset freeze and a travel ban.

Apart from the Cyber diplomacy toolbox, EU cyber security is also advanced globally and realized through the recently released Acts like NIS2, Cyber Resilience Act, and Cyber Solidarity Act. More and more the EU integrates its cyber security initiatives in its general digital diplomacy approach. That also can be understood from the Council's Conclusions on digital diplomacy. With its cyber security regulations, the EU tries to promote its vision of a global, open, stable, and secure cyberspace in multilateral, regional, bilateral, and multi-stakeholder engagements.

From the practical perspective in the diplomatic context, the EU conducts the EU Cyber dialogues. The 8th EU-US Cyber Dialogue took place in December 2022. It serves as the platform to discuss the cyber regulations from both sides as well as the commitment to work together on "promoting a global, open, free, stable and secure cyberspace where international law, including respect for human rights and fundamental freedoms, fully apply, supporting the social, political and economic development of the EU, the US and our partners, including Ukraine and Western Balkans."

The EU conducts another Cyber Dialogue with Ukraine. It was established in 2021 prior to the full-scale Russian invasion. Its objective was to work together on the promotion of rules-based cyber spaces – a similar objective to the Cyber Dialogue with the US. But in Ukraine's context, the important part of the discussion was the state of Ukraine's legislation developments including the alignment with the NIS and the other EU institutional and legislative frameworks. The Second dialogue took place in October 2022 and was focused on Ukraine's cyber resilience against the Russian cyber-attacks and the development of cyber capabilities with the EU's constant and consistent support. Among others the EU has emphasized political, financial, and material support to Ukraine to strengthen its cyber resilience, the update for the NIS2 and the implementation of Ukraine's cyber security strategy 2021-2025.

Last but not least, the EU has supported the initiative – EU Cyber Direct. It is an EU-funded project focused on policy support, research, outreach, and capacity building in the field of cyber diplomacy. It is the practical realization of the EU Cyber diplomacy at the level of experts who analyze the global trends in cyber security as well as engage in the promotion of the EU files in the multilateral fora.

3. Digital/cyber/ tech diplomacy: the case of Ukraine

With Russia's full-scale invasion after 9 years of war, technologies, modern infrastructure, and cyber resilience have only proven the benefits and importance of digital transformation – the foundation of Ukraine's resilience.

3.1 Digital diplomacy

Digital diplomacy in Ukraine was first mentioned as part of the public diplomacy strategy adopted in 2021 by the Ministry of Foreign Affairs of Ukraine. It is defined as the dimension of public diplomacy, which involves the use of digital technologies and platforms, as well as interaction with them to protect the country's national interests. The dimensions of work were determined as follows:

- Interaction with international digital platforms to promote a positive image of Ukraine in the world and protect national security.
- Using digital tools to organize public diplomacy events and projects.
- Using the potential of social networks and interaction with online communities to form a positive image of Ukraine and promote Ukraine's interests in the world.

To achieve the goals, the objective was to strengthen relations and cooperation with large technological companies through the establishment of cooperation between the Ministry of Digital Transformation, diplomatic institutions, and international digital platforms.

Comparing it to the EU approach to digital diplomacy, the difference is clear. Although the strategy defines the protection of the national interest as its goal, Ukraine has always perceived the role of digital diplomacy in terms of the communication instrument – for the promotion of the positive brand of Ukraine. But what is important, Ukraine has set the goal to promote its image as a digital country but not to increase its power through the promotion of its technologies and digital capabilities, like for example Diia.

DIGITAL DIPLOMACY HAS LONG TIME AGO BECOME MORE THAN JUST A SET OF COMMUNICATION TOOLS.

If we compare the institutional structure of Ukraine with the EU in the question of who should deal with digital diplomacy and issues of the geopolitics of technologies, then a question arises not only at the level of strategy but also at the level of institutions. If digital diplomacy in the EU is led by the EEAS and supported by the work of DG CNECT, in Ukraine it is the opposite. The Ministry of Foreign Affairs promotes Ukraine's interests via communication products and companies including Ukraine.ua, which has recently achieved the outstanding result of 1 million of followers on Instagram. At the same time, the Ministry of Digital Transformation is the contact point for the development of international cooperation in the field of technology governance while developing domestic digital policy.

With the start of the full-scale invasion, Ukraine has started to actively engage in global technology governance issues while at the same time fostering and enhancing relations with its main partner in the digital policy – the EU.

- **Multilateral cooperation: global context**

In the international context, the USA and the EU actively tried to establish their principles of Internet regulation by publishing the Declaration on the Future of the Internet in April 2022. Ukraine became one of the signatories, which shows commitment to Western European principles and standards.

Another example of international cooperation is the participation of Ukraine in the G7 Digital and Tech Ministers' Meeting 2023 in Japan. The Ukrainian delegation was represented by Valeria Ionan, Deputy Minister of Digital Transformation for European Integration. The Ukrainian Deputy Minister shared the Ukrainian experience and promoted Ukraine's best practices in the stages of creating a 'state in a smartphone' through a unique Diia product. But the G7 first of all focuses it further work on the G7 Action Plan for Building a Secure and Resilient Digital Infrastructure, promotion of the principles of the Declaration on the Future of Internet, making visible and tackling the tactics of digital authoritarianism, securing the supply chains and the application of the emerging and developing technologies (EDTs), promotion of human-centric and trustworthy AI based on the OECD AI Principles. All of these issues should be on Ukraine's agenda.

At the UN level now Ukraine needs to engage in two important aspects. First – is the cooperation with the International Telecommunication Union (ITU). In March 2022, ITU adopted the Resolution 1408 of the ITU Council on assistance and support to Ukraine in rebuilding its telecommunications sector. The second aspect is the global work on the UN Cybercrime Convention that might be designed in 2023 in the draft version by the UN Cybercrime Treaty Adhoc Committee and where Ukraine needs to increase its voice and presence.

- **Cooperation with the EU and its support to Ukraine**

At the bilateral level, the EU is still the main partner for Ukraine, especially given the fact that Ukraine received the status of a candidate for EU accession in June 2022. Ukraine is actively approaching integration into the Single Digital Market within the framework of fulfilling the requirements for EU membership. The EU in turn has provided significant support to Ukraine through the following initiatives:

- **Implementation of the eIDAs.** In April 2023 The European Commission also recognized that Diia.Signature-EUcomplies with the EU's eIDAS regulation and can be used to sign documents or contracts valid in both Ukraine and the EU. For its part, Ukraine has already recognized EU-qualified trust services. This allows EU citizens to use their national qualified certificates for electronic signatures or seals in Ukraine or when doing business with companies in Ukraine. Now the EU works on the eIDAS regulation to make possible cross-border e-ID a reality. The European Commission works closely with the Ministry of Digital Transformation of Ukraine. Diia is also the case where Ukraine can share its experience with the EU and promote its approach in the design of the Digital ID that the EU is only planning to introduce in 2024.
- **Access to EU roaming space**. On April 8, 2022, the European Commission and the Parliament supported the joint statement of EU operators and Ukrainian operators regarding the provision of free accommodation and free calls from abroad to Ukraine. This agreement was extended at the end of July and in 2023 – for another 6 months. Moreover, the European Commission also authorized the national regulatory body of Ukraine to participate in BEREC – the Body of European Regulators in the Field of Electronic Communications. Last, in April 2023, The EU Council and the European Commission supported Ukraine joining the free-roaming agreement with the EU on a permanent basis, the ministry stressed. For this, the European Commission has proposed to include provisions on roaming in Annex 17-3 of the EU-Ukraine Association Agreement. The

Council of the European Union has approved this proposal. Now it is up to the EU-Ukraine Association Committee to approve and for Ukraine to implement.

- **Support of digital projects in Ukraine.** In September 2022, the European Commission signed an agreement on the accession of Ukraine to the Digital Europe Program. Ukrainian enterprises, organizations, and public administration bodies will be able to benefit from the program's funding and support in areas such as supercomputers, artificial intelligence, and digital skills. They will also be able to participate in Digital Innovation Centers – one-stop centers that help companies dynamically respond to digital challenges and become more competitive.
- **Launch of the "Laptops for Ukraine" program,** which aims to collect and deliver laptops, smartphones and laptops to schools, hospitals, and state administrations in the most war-affected regions of Ukraine. So far, the Commission has helped deliver 12,000 donated devices to Ukraine through the EU Civil Protection Mechanism.

3.2 Tech diplomacy

In Ukraine's context, tech diplomacy can be defined in a separate context considering the large number of partnerships with foreign private companies, including Big Tech and the strong need for them in the war context. But even before the full-scale invasion Ukraine's cooperation with private companies in the digital policy has increased with the need to deploy 5G networks. Big Tech companies have also been of interest to Ukraine for a long time. Since the full-scale invasion, partnerships with private companies have become the rescue tool for Ukraine's tech and cyber capabilities because of the emergency and flexible approach of the companies. The establishment of public-private cooperation with foreign companies was aimed at strengthening the technological and cyber capabilities of Ukraine in the war and at the same time depriving Russia of technological advances. These goals directly serve Ukraine's foreign policy interests in wartime to protect its national sovereignty and develop partnerships for global dialogues and support.

- **Connectivity**

Significant work had been carried out on the implementation of 5G infrastructure in Ukraine before the full-scale invasion. In 2020, a memorandum of cooperation was signed between the Ministry of Digital Transformation and Ericsson. Basically, the parties agreed to cooperate on the development of fixed and mobile communication systems of the new generation 4G (LTE-Advanced) and 5G for further informatization of the country and increasing the digital potential of civil society. Ukraine also cooperated actively with the Chinese company Huawei. In October 2020, the State Service for Special Communications and Information Protection of Ukraine signed a memorandum of cooperation with Huawei in the fields of cyber security, cyber protection, and telecommunications. The Minister of Foreign Affairs Dmytro Kuleba immediately criticized the initiative as it was done without coordination with the MFA. According to the "Economic Truth" this was done because of the news stating that Western partners were surprised by Ukraine's choice of partner. That was the first and the last public case in Ukraine when the MFA engaged in the context of partnerships on technology implementation. After that, the information about this memorandum was deleted. This once again confirms that the factor of geopolitics affects the country's digital policy and vice versa. While the European Union is on the path of limiting the influence of other actors and companies on critical infrastructure based on the risk-based approach, that should be also the approach of Ukraine in the context of European integration.

Another case comes for the most prominent example in times of war concerning connectivity – Mykhailo Fedorov's address on Twitter to Elon Mask and the use of Startlinks in Ukraine. After 12 hours Musk replied on the social media platform saying "Starlink service is now active in Ukraine." Despite his mixed position after several months of the war, Starlink satellite Internet services still

provide critical access to the Ukrainian government, the Armed Forces, and rescue services to the satellite Internet. As of March 2023, the number of Starkinks in Ukraine has reached 42 000. Ukraine spends no funds on their use – Space X provides the technical maintenance, and like-minded partners provide the funds. That's the case of how partnerships can be important, especially when the private partnership with tech companies is reinforced by the support coming from other counties. Although there were messages from the company about not accepting any use of Starlinks for piloting drones and carrying out offensive capabilities. Moreover, Russians try to disrupt Starlink's transmissions in Ukraine via their Tobol electronic warfare systems. Thus Ukraine needs to evaluate two risks in terms of connectivity – protection of its infrastructure and avoidance of the significant dependency on one foreign technology.

- **Artificial Intelligence**

The similar situation to connectivity comes to the application in Ukraine of Artificial intelligence technologies of the US company – Clearview AI. From the start of the invasion Ukraine was using the Clearview AI face-recognition technologies to detect the Russians who commit crimes in Ukraine. But in April 2023 the Minister of digital transformation communicated that cooperation with the Clearview AI will be fostered. As of this time, 14 Ukrainian governmental authorities use the technology. Among the ideas where AI can be further integrated are the customs system and banking. The company is planning to test new products in Ukraine and even open its office with a local team of developers. But there is a big "but". The company has been repeatedly accused of violating human rights – especially the right to privacy. France has fined the company 20 million euros according to article 83 of the GDPR as the company had no legal rights to collect the data of French citizens. In Sweden police were fined by the country's data regulator for using Clearview's offerings to "unlawfully" identify citizens. That's why the further promotion of cooperation with the company is of great concern for the rights of citizens and for the integration of technologies in critical information infrastructure and the provision of digital services. The foreign media already mention that Ukraine uses the Clearview AI technologies of face-recognition at the "human rights cost".

- **Big Tech companies support and 'Digital blockade'**

Lots of companies were the first to offer help and cooperation without even Ukraine requesting. Microsoft has continued at the end of 2022 to provide additional technology aid valued at roughly $100 million, which will ensure that government agencies, critical infrastructure, and other sectors in Ukraine can continue to run their digital infrastructure and serve citizens through the Microsoft Cloud. Google provided Ukraine with 15 million in aid, expanded the scope of Project Shield, which protects more than 150 Ukrainian sites from DDoS, and launched a system of air alert notifications for Android users. The company is also providing critical cybersecurity and technical infrastructure support by making a new donation of 50,000 Google Workspace licenses for the Ukrainian government so that to ensure Ukrainian public institutions have the security and protection they need to deal with constant threats to their digital systems. Recently Google in cooperation with the Ministry of Digital Transformation of Ukraine and East Europe Foundation launched a large education project for upskilling and re-skilling – Diia. Education. Last but not least, in May 2023, The Ministry of Digital Transformation signed the Memorandum on cooperation with the American corporation IBM in order to join efforts on the development of AI technologies, a search for cloud solutions for the support of Ukraine's digital infrastructure, strengthening of cyber security and increase digital skills of Ukrainians.

But what Ukraine has been advocating and working on since the first days of the invasion is the campaign of the "digital blockage" of Russia. Sanctions imposed by the US and the EU on Russia, including the digital and technological spheres, have given the green light to many companies to participate in the war on the side of Ukraine. As for other companies, Apple stopped placing its products in the Apple Store in Russia, and also cut access to the Apple Pay system. Microsoft left the leading Russian company VK without access to Microsoft services, harming the work of the main mail service - Mail.ru. As for the main telecom providers in Russia, Nokia and Ericsson

stopped deliveries to Russia and suspended 5G deployment. In the past, Russia was reluctant to hang on to the telecommunications company Huawei, fearing dependence on China, but now it is the most obvious partner.

Semiconductors are another technology that needs to be considered seriously. Semiconductors are key elements to produce advanced weapons, automobiles, and digital technology. At the beginning of the invasion AMD and Intel, Qualcomm – a well-known semiconductor manufacturer, stopped all sales of products to Russia and Belarus considering the US sections against the Russian defense industry. Taiwan's largest semiconductor company TSML and South Korea's Samsung have done the same. The EU with its 10 packages of sanctions has sharpened and extended export controls on dual-use goods to target sensitive sectors in Russia's military-industrial complex, and has limited Russia's access to crucial advanced technology. But at the same time, despite Western sanctions, foreign-made technology continues to find its way into Russia's war machine according to the analysis of Carnegie Europe. Russia's most consequential partner, China, has extended a critical helping hand to an increasingly isolated Russia, funnelling over $500 million worth of microelectronic components needed to manufacture military gear into Russia's defense industrial base in 2022 alone.

3.3 Cyber Diplomacy

The concept of cyber diplomacy is not mentioned by the MFA in the public diplomacy strategy. But Ukraine's Cyber Security Strategy of 2021 stipulated the need for an element of Ukraine's participation in international cyberspace and the spread of its own interests on international and European platforms, including the establishment of closer contacts with international stakeholders.

In 2022 Ukraine has proved to be resilient against 2194 Russian cyber-attacks in the last year. The EU has constantly supported Ukraine in its cyber resilience. Days before Russia's invasion, the Lithuanian defense ministry announced the deployment of an EU Cyber Rapid Response Team (CRRT); a project born from EU military cooperation. The 8 to 12 cybersecurity experts from EU countries like Estonia, Poland, and Romania assist Ukraine's cyber defense in defending its networks.

In March 2022, Ukraine joined the Cooperative Cyber Defence Centre of Excellence, a Nato-accredited institution focused on cyber defense research. Sharing "threat indicators" and joint training exercises for cyber defense specialists are crucial according to the head of the SSSCIP. In the newly issued in April 2023 Decree of the Cabinet of Ministers of Ukraine on the approval of the Action Plan on the realization of the Strategy on the Foreign policy Ukraine among all goals indicates joining EU's PESCO projects, the conduct of the new Cyber Dialogue with EU and deepening of the cooperation with ENISA in the cyberspace. Furthermore, cyber security and dialogues are mentioned in the goals for cooperation with the US, the UK, and the Lublin triangle states. Ukraine in such cooperation shall take advantage of its experience and build a separate dimension – cyber diplomacy

4. Conclusions and recommendations

4.1 EU: regulations and cooperation with like-minded partners

Innovations that are at the core of digital and tech policy define global competitiveness and the way the actors engage both in bilateral and multilateral relations. The US, China, and the EU – all have incorporated in its foreign policy digital and tech policies as the instrument for the promotion of interests and values. Actors complete the establishment of the rules at the geopolitical technological roundtable. The EU has its important seat.

EU'S DIGITAL AND CYBER DIPLOMACY BASED ON SOLIDLY SHAPED REGULATIONS IS AIMED AT THE PROMOTION OF ITS OWN RULES THROUGH COOPERATION WITH LIKE-MINDED PARTNERS AT DIFFERENT LEVELS.

- **Digital diplomacy.** To understand the EU's digital diplomacy, one needs to understand its digital policy files – Digital Markets Act, Digital Service Acts, Data Governance Act, EU Chips Act, and especially AI Act, which the EU puts as a priority the global regulatory leader. The EU creates bilateral platforms for dialogues, like Trade and Tech Councils, and Digital Partnerships. Last, it supports regional initiatives and provides funds for digital transformation in developing states. Bilateral partnerships, of which crucial is the EU-US one helps to form coalitions for the EU to promote existing multilateral platforms of democracy and human-centered technology regulations.
- **Tech diplomacy** – partnerships with the Big tech companies. The EU is the one that strives to reduce its dependencies on other countries and foreign private companies and at the same time supports its domestic businesses and initiatives with regulatory Acts, for example, such as EU Chips Act, EU Cloud Certification Scheme, etc. But it's also essential in times of interdependencies not to underestimate the need for cooperation with private companies via the fostering of tech diplomacy. For this, the EU has opened an office in San Francisco, while in Brussels Big tech companies are part of the constant discussions on the regulations.
- **Cyber diplomacy.** The EU was among the first to establish the Cyber Diplomacy Toolbox and recognized the importance of cyberspace for foreign policy initiatives. Thus the EU has legitimized the use of restrictive measures for cyber attacks carried out against the EU and Member states. Moreover, the EU has developed a solid regulatory framework to increase the cyber resilience of critical infrastructure (NIS2), and businesses (CRA), and to shape the coordinated response mechanisms at the EU level while enhancing the need for the development of cyber skills (EU Cyber Solidarity Act). The EU also uses the instruments for cooperation – Cyber Security Dialogues to ensure it is on the same page with like-minded partners. Last, the EU supports the non-governmental Cyber Direct initiative which is actively involved in tracking global tendencies on cyber security and advocates for the EU. All these initiatives serve the global priorities of digital diplomacy where cyber diplomacy is an integral part.

4.2 Ukraine: flexibility, speed, and cooperation with multiple actors

As mentioned above, the full-scale invasion prompted Ukraine to re-evaluate the role of technologies and both private and public partnerships in the digital domain.

ALTHOUGH UKRAINE'S DIGITAL DIPLOMACY HAS BEEN FORMED BY THE EMERGENCY SETTINGS, UKRAINE IS CONSISTENT IN ITS COOPERATION WITH THE EU ON THE DIGITAL POLICY.

It has achieved significant progress both in the implementation of the EU's acquis and up to the addition of the amendments to the Association Agreement with roaming provisions. As the EU digital policy is constantly developing, Ukraine needs to consider two things. First, the implementation of the EU digital and cyber regulatory acts is a constant-moving target that requires consistency and close coordination with the EU. Second, Ukraine needs to consider not only how to implement the EU digital policies, but how to promote its own best practices at the EU level and adjust the EU files to the national context.

At the domestic level, Ukraine has a number of the best practices of resilience in cyberspace, the use of technologies in the war, and the development of the Diia. Ecosystem aimed at making Ukraine the most convenient digital state in the world. Furthermore, Ukraine's resistance in the war at the digital frontline has shaped the interests of other states and the leading world media to its way of 'getting things done' at digital and cyber policies.

UKRAINE HAS DEVELOPED A NUMBER OF BEST PRACTICES THAT IT HAS ACTIVELY STARTED TO PROMOTE AT THE BILATERAL, REGIONAL, AND MULTILATERAL LEVELS OF COOPERATION.

- **Digital policy.** With its Diia product, Ukraine is recognized as the leader in e-governance solutions. In January 2023, Estonia launched the mRick mobile app based on Diia's code and UX/UI design approaches. Cooperation with Estonia has become the precedent to develop and spread Ukrainian technologies in other counties. In this regard, USAID – the American support program will provide support for at least 650,000 US dollars to spread the Ukrainian standard of e-government in other countries. In general, as of the beginning of 2023, 5 countries have already expressed their desire to make applications in their countries using the Prototype of Diia. Only at this stage, the Ukraine Vice Prime Minister and Minister of Digital Transformation admitted that Diia has become an element of Ukraine's diplomacy - "This is the brand of Ukraine, this is our reputation, this is the development of our political influence". In May 2023 Ukraine conducted the Diia. Summit in Washington. Moreover, Diia is also the case when Ukraine can share the experience with the EU and promote its approach in the design of the Digital ID that the EU is only plan to introduce in 2024 and then the work will have to be done on the mutual recognition of the EU and Ukraine's digital IDs.

- **Tech diplomacy.** Ukraine is an example of how private-public partnerships can be the foundation of resilience in many aspects of digital policy. Partnerships with foreign private companies, the speed of Ukraine advocating and getting support was enormous as required by the war circumstances – from getting Starlinks to the recent signing of the memorandum

with IBM. Flexibility, quick and targeted requests - that's the approach of Ukraine to its tech diplomacy.

- **Cyber security.** Since 2014 Ukraine has obtained practical experience of how to deal with cyber-attacks being the so-called 'test-place' for Russia. Ukraine has done a number of initiatives to safeguard its cyber resilience with the full-scale invasion – the creation of a layered system of cyber defense for the state IT infrastructure, relocation of equipment and database backups to safer areas of Ukraine, creation of the cloud data storages and backs at other states, etc. Ukraine needs to promote this experience. While Ukraine still needs to do lots of work on the implementation of EU regulations on cyber security including the new ones, the EU, for example, took Ukraine's practice into its EU Cyber Solidarity Act released in April 2023 that establishes the new EU Cybersecurity Reserve consisting of incident response services from trusted providers pre-contracted and therefore ready to intervene, at the request of a Member State or Union Institutions, bodies, and agencies, in case of a significant or large-scale cybersecurity incident.

4.3 Recommendations for the EU on increasing its regional engagement in EaP countries, including Ukraine

Digital diplomacy:

- The EU needs to actively start the discussion at the level of the Association Committee and expert network on the need for Ukraine and the EaP states to follow the developments regarding the recent EU regulatory digital and cyber acts and consider the fast-coming alignment with them.
- The EU also needs to involve the policymakers in the EaP states and the expert network in the discussions on the geopolitical digital and technology agenda.
- it is important for the EU to Include in the dialogue with the EaP states the discussion on the risk-based approach to the development of partnerships with foreign private companies that integrate their technologies into critical information infrastructure and security systems. Although the candidate countries actively follow the EU integration agenda, it does not limit the influence and incorporation of China in the EaP region.

Cyber Diplomacy:

- The EU can establish Cyber dialogues with other states in the EaP region to be able to track the progress in the implementation of cyber policies and check out the emerging cyber threats.
- The EU may enhance cyber security cooperation and provide more support via its mission in Moldova - EUPM and in Ukraine - EUAM where in the latter the mission already supports the projects on online safety.

- The EU is to continue to support Ukraine in its digital transformation and strengthen its cyber resilience in times of war as its cyber security is also dependent on the cyber security in Ukraine and in the region.

4.4 Recommendations for Ukraine on shaping its digital, cyber and tech diplomacy

Although the Russian invasion of Ukraine has made digital diplomacy an emergency tool, Ukraine needs to develop a consistent approach to it with the EU principles of democracy-technology nexus in its core.

UKRAINE SHOULD FOCUS ON THE DESIGN OF THE UPDATED STRATEGY ON DIGITAL DIPLOMACY, INSTITUTIONAL CAPACITY-BUILDING, AND RISK-BASED APPROACH TO PARTNERSHIPS.

Digital diplomacy:

- The Ministry of Foreign Affairs of Ukraine (MFA) should engage in a comprehensive dialogue with the Ministry of Digital Transformation (MinDigital) to understand the situation of Ukraine's engagement in global technological governance and the partnerships that Ukraine has built with private companies. The dialogue between the MFA and Mindigital shall result in a clear division of the functions between the 2 institutions on digital diplomacy. Ukraine has the opportunity to build a sustainable and strategic institutional model similar to the one that exists in the EU: with the Vice Prime Minister leading Ukraine's digital policy development and priorities while the MFA shall on a daily basis assist in its externalization according to the foreign policy priorities with the support of the Ministry of Digital Transformation.
- At the level of the MFA, Ukraine still perceives digital diplomacy only through the prism of communication tools and as a part of public diplomacy. Thus the Ministry needs to start the work on the updated strategy for digital diplomacy recognizing its importance in the work of the diplomats and the diplomatic representations overall for the achievement of the foreign policy goals. The updated approach of the MFA toward digital diplomacy should include the mapping of the current existing opportunities for cooperation in the digital domain at bilateral, regional, and multilateral levels and advocate for new platforms for engagement with like-minded partners in the way the EU does.
- The MFA should have the responsible official position for the performance of digital diplomacy which would establish the link between the MFA's coordination with the Vice-President, Ministry of Digital Transformation, diplomatic representations, and external partners. The Chief Digital Transformation Officer (CDTO) is responsible for internal processes and needs to be also engaged in the external dimension. Or Ukraine might follow the example of Denmark and many other states and appoint a digital ambassador who will deal with the portfolio of digital diplomacy and will coordinate and implement work in this regard.
- Following the EU's examples, MFA in cooperation with the Ministry of Digital Transformation needs to conduct training for diplomats on the basics of digital policies, geopolitics of technologies, and online safety skills so that to make sure Ukraine's digital diplomacy serves Ukraine's foreign policy goals.
- Ukraine needs to continue actively to promote its best practices regarding the Diia ecosystem at all possible levels: global, regional, and bilateral. It is an example of products-oriented digital diplomacy and it needs to continue to be externalized in other states. But in terms of its promotion, more and more questions from partners will be raised about the security standards of Diia, the data protection regulations, data infrastructure, etc. Thus Ukraine needs to be ready for these questions. Global and EU agendas are much more enrooted in the regulations rather than products and Ukraine needs to consider it. The narrative needs to be changed from "building the most convenient digital state", to "building the most convenient safe digital state".

- More expert discussions and research in Ukraine should take place on digital diplomacy, and the use of the technologies in Ukraine for achieving its domestic and foreign policy goals. Moreover, the Ukrainian expert network shall follow the discussions around the EU-US Trade and Tech Council to understand the transatlantic narratives and work on the digital and technology governance.

Tech diplomacy:

- Tech diplomacy shall be included in Ukraine's updated digital diplomacy strategy as one of the tools – the establishment of sustainable public-private partnerships with foreign tech companies. But Ukraine needs to apply the EU approach to the development of private partnerships based on the evaluation of the security and dependencies' risks. The application of Chinese technologies which are limited in Europe because of the violation of human rights can affect Ukraine's relations with the European Union, especially in the context of European Integration. In cases of connectivity infrastructure and AI, the EU's regulations based on the risk-based approach should be taken into consideration in Ukraine when it comes to cooperation with foreign companies. Ukraine needs a full audit of the private technologies used in governmental institutions, especially in the security sector.
- The MFA in cooperation with MinDigital shall actively promote further relations and cooperation with Big tech companies, including the engagement of Ukraine's diplomatic representations.
- It is important for Ukraine to continue to realise the campaign of the "digital blockade" of Russia and engage in the dialogue with the EU on the state of the implementation of the Member States' export-related restrictions on dual-use technologies to Russia.

Cyber diplomacy:

- The MFA, Mindigital, SSSCIP, and the National Cyber Coordination Centre need to develop a joint approach towards the cyber diplomacy strategy that can be part of the generally updated digital diplomacy strategy or be the separate one with the view to Ukraine's needs.

- This approach must include a clear division of institutional responsibilities on external engagement on cyber issues, alignment with the EU's current cyber security regulations, and mapping of the opportunities for strengthening the cooperation with like-minded partners on cyber security, resilient infrastructure, and security of supply chains.
- The cyber resilience of Ukraine is the best practice that Ukraine needs to promote at international conferences and multilateral platforms for discussions. Moreover, the expert network shall actively participate in the realization of cyber diplomacy - similar to the work of the EU Cyber Direct initiative.
- Ukraine also needs to actively participate in the design of the UN Convention on Cybercrime calling for the prosecution of Russian cybercrimes in the war against Ukraine.

INTERNATIONAL RENAISSANCE FOUNDATION

UKRAINIAN PRISM

EU'S AND UKRAINE'S APPROACHES TO DIGITAL DIPLOMACY IN THE GEOPOLITICS OF TECHNOLOGIES

The research is conducted by the Foreign Policy Council "Ukrainian Prism" as a part of the project supported by The International Renaissance Foundation.

Authour:
Viktoriia Omelianenko, Expert of Ukrainian Prism Europe,
co-founder of NGO MINZMIN

info@prismua.org
http://prismua.org/en/
/PrismUA