The Kosciuszko Institute

PARTNERS:

CYBERSEC
EUROPEAN CYBERSECURITY FORUM

comCERT

THE TWILIGHT OF THE NEUTRALITY OF DIGITAL TECHNOLOGY

MACIEJ GÓRA, EWELINA KASPRZYK, ELIZA KOTOWSKA, MICHAŁ KRAWCZYK

EDITOR: PAWEŁ OPITEK

The Kosciuszko Institute

THE TWILIGHT OF THE NEUTRALITY OF DIGITAL TECHNOLOGY

AUTHORS:

Maciej Góra – Analyst and Project Manager, the Kościuszko Institute

Ewelina Kasprzyk – Programme Director, the Kościuszko Institute

Eliza Kotowska – Junior Researcher and Project Manager, the Kościuszko Institute

Michał Krawczyk – Analyst and Project Manager, the Kościuszko Institute

Edited by: dr Paweł Opitek – Prosecutor at Public Prosecutor's Office, Cybersecurity Expert at the Kościuszko Institute

Proofreading: Justyna Kruk

Layout and DTP: Wiktoria Konieczniak – Creative Manager, the Kościuszko Institute

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10,
31-130 Krakow, Poland
Phone: +48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

TABLE OF CONTENTS

INTRODUCTION

The Ukrainian-Russian conflict, which has been ongoing since 2014 and the illegal seizure of Crimea by the Russian Federation, abruptly escalated on 24 February 2022 with a force not seen in Europe since the World War II. 80 years after the greatest battles of the Eastern Front, the same areas of Ukraine have once again become a theatre of warfare played out on land, on sea and in the air. **But this war is also being fought in new military domains, targeting elements in outer space and cyberspace. Moreover, the participants in this conflict are no longer just states, but also new, powerful, international players – technology corporations[1].** Their support to Ukraine's cyber defence has proven to be critical to allow the country to successfully resist Russian cyberattacks. But the aforementioned companies have a much broader impact on the conduct of the war. They not only help ensure a safe operation of critical infrastructure, but also provide military technology designed directly or indirectly for warfare (e.g., satellite reconnaissance, communications systems) and civilian technology to support the economy (e.g., the international SWIFT system). Online social media platforms, in turn, serve as forums for discussion and exchange of views among their users, thus shaping public opinion and preventing disinformation. This aid has been welcomed by the international community and especially by Ukrainians themselves, who emphasise how crucial this support is for their independence and sovereignty.

However, the wartime activism of technology suppliers has serious ramifications, not only for the outcome of the Ukraine conflict. It is necessary to consider the legal, operational, and strategic implications that this shift in the geopolitical arena presents. How should decision-makers respond to the twilight of neutrality of digital technology providers? Is this the new age of enhanced, geopolitically motivated corporate social responsibility? How will the tech providers' rise to prominence project into the next decades of the 21st century?

This policy brief examines these questions in detail, looking at the ways in which western technology corporations have helped Ukraine in its fight against Russia, and the potential implications of this assistance. It will also consider the potential benefits and drawbacks of this aid, explore political and societal implications of it, and offer recommendations on how to address the challenges and concerns that have arisen as a result of this support.

1 This policy brief deals exclusively with technology companies and their activity during the war in Ukraine. Any use of the words 'corporations' and their synonyms including 'companies', 'business' and 'firms', refers to private sector companies from the technology industry, unless stated otherwise.

RUSSIAN CYBER OPERATIONS AGAINST UKRAINE 2014–2021

The way Russians support their geopolitical agenda with cyber operations could already be seen during the first stage of the Russian-Ukrainian conflict. As Nikolay Koval, acting at the time as the head of Ukraine's CERT (Computer Emergency Response Team), writes 'the number and severity of cyber-attacks against Ukraine rose in parallel with ongoing political events.'[2] Following the Russian military incursion into Crimea on 2 March 2014, the mobile phones of Ukrainian parliamentarians were hacked, while the Ukrainian government's website was inaccessible for 72 hours[3]. In May of the same year, during the Ukrainian parliamentary elections, hackers from the Russian CyberBerkut group broke into the systems of the Ukrainian Central Election Commission, disabling the vote-tallying system. Hackers then unsuccessfully tried to interfere with the outcome of the voting by announcing the victory of the leader of the Right Sector, a far-right political formation,

2 N. Koval, *Revolution Hacking*, [in]: K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, https://ccdcoe.org/uploads/2018/10/Ch06_CyberWarinPerspective_Koval.pdf, p. 57

3 T. Maurer, *Cyber Proxies and the Crisis in Ukraine*, [in]: K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, https://www.ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf, p. 81

Dymytro Yarosh, in the elections[4].

Years 2015 and 2016 were filled with notorious cyberattacks on the Ukrainian critical infrastructure. Russian hackers managed twice to briefly deprive hundreds of thousands of Ukrainian residents in the Ivano-Frankivsk and Kyiv regions of electricity by infecting the digital systems of energy suppliers Prykarpattyaoblenergo and Ukrenergo with malware[5]. Between 27 and 28 June 2017, the day before the Ukrainian national holiday, NotPetya, malware created from a combination of the ransomware Petya and a set of EternalBlue vulnerabilities, hidden in an update to the MeDoc accounting software, paralysed dozens of Ukrainian state agencies and private organisations. But the wiper malware did not stop there. Posing as ransomware, it spilled over outside Ukraine, causing billions of dollars in losses worldwide[6]. In 2020, the Security Service of Ukraine reported that it had prevented 482 attacks targeting critical infrastructure[7], while the National Coordination Center for Cybersecurity under the National Security and the Defense Council of Ukraine stated in a press release that it had recorded about a million of different cyber incidents in Ukraine, including application layer attacks, scanning attempts, website attack attempts, phishing, DDoS (Distributed Denial of Services) attacks, spread of malicious software, and more[8]. **Given the long history of Russia using its cyber capabilities to target and disrupt its adversaries not only in Ukraine, but also in NATO and the European Union, highly qualified but limited cyber defence resources that Ukraine possessed, as well as the fog of war surrounding Russian cyber military doctrine, many analysts expected that if a full-scale war had broken out, it would have likely turned a very large cyber dimension, possibly turning into the first cyberwar.**

4 *Ukrainian parliamentary election interference (2014)*, https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014)

5 *Rosyjska cyberofensywa na Ukrainie, czyli czego spodziewać się już dziś?*, https://sekurak.pl/rosyjska-cyberofensywa-na-ukrainie-czyli-czego-spodziewac-sie-juz-dzis/

6 A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

7 V. Kremez, *Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting*, https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

8 *About a million cases of cyberattacks and cyberthreats recorded in Ukraine this year*, https://www.ukrinform.net/rubric-defense/3077855-about-a-million-cases-of-cyberattacks-and-cyberthreats-recorded-in-ukraine-this-year.html

2022 – THE CYBERWAR THAT NEVER WAS

The cyber operations were a prelude to a 2022 full-scale military operation launched by the Kremlin. As tensions failed to de-escalate through diplomatic efforts, Russian hackers changed the type of their cyber operations from CNE-type (Computer Network Exploitation; action taken to make use of a computer or a computer network and the information hosted therein in order to gain advantage)[9] to CNA-type (Computer Network Attack; action taken to disrupt, deny, degrade or destroy information resident on a computer and/or computer network, or the computer and/or computer network itself)[10] attacks, using destructive wipers designed to destroy victim's data without the ability to restore it. On the eve of the invasion, a malware called HermeticWiper AKA FoxBlade was deployed in order to 'destroy roughly 300 systems across more than a dozen government, IT, energy,

9 *computer network exploitation*, after: *NATO Glossary of terms and definitions (English and French)*, https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

10 *computer network attack*, after: *NATO Glossary…* op.cit.

Graphic 1. Map of coordinated Russian cyber and military operations in Ukraine.[11]

agricultural, and financial sector organisations in Ukraine'[12]. On the day of the attack, an hour before Russian tanks crossed the Ukrainian border, the Russians attacked KA-SAT, a satellite network owned by a U.S. company Viasat, which resulted in 'a really huge loss in communications'[13], as stated by Viktor Zhora, Chief Digital Transformation Officer at the State Service of Special Communication and Information Protection of Ukraine. During the next stages of the war, several cyber operations were linked to kinetic operations performed by the Russian military.

After the failed attempt to seize Kyiv, and shifting the burden of fighting to eastern Ukraine, infrastructure once again became the main target[14]. However, the cyber operations on infrastructure were less impactful than many had feared. There may be several explanations for this phenomenon: poor preparation of cyber operations on the Russian side, a lack of cohesion between Russian ground troops and state-sponsored hackers focusing primarily on intelligence activities, and the Ukrainians' effective cyber defence. The latter results

11 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, p. 9

12 Microsoft Digital Security Unit, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, p. 7

13 *Lessons from Russia's cyber-war in Ukraine*, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine

14 D. Ignatius, *How Russia's vaunted cyber capabilities were frustrated in Ukraine*, https://www.washingtonpost.com/opinions/2022/06/21/russia-ukraine-cyberwar-intelligence-agencies-tech-companies/

from many overlapping factors, such as the prowess of Ukraine's thriving IT sector, the modern and mature digital policy of the government of President Volodymyr Zelensky, a significant assistance of Ukraine's government partners, especially the U.S. and the United Kingdom and, perhaps most of all, a significant and extensive help of the private sector.

PRIVATE SECTOR INVOLVEMENT IN CYBER DEFENCE OF UKRAINE

With the end of the Cold War and the reduction of state budgets for arms spending, the involvement of private actors in the defence sector has increased significantly, marking a new era in the government-business relationship[15]. The once clear-cut distinction between military, dual-use and civilian applications is increasingly blurred with the advent of the Internet-enabled globalization, the crucial role that technology companies play in building digital infrastructure and the rise of cyber as a military domain.

In 2022, we observed the private sector engaging in a wide range of activities in response to the Russia-Ukraine conflict, from supporting Ukraine's defensive capabilities, to enabling the continuity of functioning of the state institutions and critical infrastructure, and finally to donating funds and launching charity initiatives. Regardless of the magnitude, severity and outcome of the measures taken by the companies, their actions can be grouped into the following categories:

1. Backing out of Russia (and Belarus),

15 W. Chin, *Technology, war and the state: past, present and future*, International Affairs, 95(4), 765–783. doi:10.1093/ia/iiz106

2. Enabling and extending services to Ukraine,
3. Threat intelligence sharing,
4. Financial support.

The private sector has been helping Ukraine by ceasing their business operations in Russia and Belarus. This type of engagement is more than just a symbolic way of showing support for Ukraine and condemning the war. By cutting ties with Russia, businesses are affecting both the Russian economy and its position in the international order. Companies like Intel and LG Electronics stopped shipments to customers located in Russia and Belarus while IBM and Ericsson suspended all of their operations in Russia[16]. Visa and Mastercard no longer work in Russia and are restricted in Belarus[17] and Apple and Microsoft have both stopped selling their products in Russia[18]. These are just a few examples in a sea of many. Such measures weaken the Russian economy as the country loses contracts with profitable companies. Furthermore, Netflix and Disney have cancelled any future productions and projects which were to take place in Russia. **Aside from affecting the economy, this sends a powerful message that Russia is not seen as a legitimate partner. This lack of collaboration weakens Russia's position in the international system, increases its isolation and works to further destabilize the country's economy.**

As the war goes on, the private sector continues to support Ukraine by providing services and equipment both in the cyber realm and on the ground. The attack on the KA-SAT network at the start of the war, for instance, highlighted the significance of satellites in the conflict. At the public request of Mykhailo Fedorov, Vice Prime Minister and Minister of Digital Transformation of Ukraine, Elon Musk sent over Starlink satellite terminals which have been crucial for maintaining communication for both military and civilians. CISCO has been providing Ukraine with various cybersecurity products while Maxar shared satellite imagery. To further strengthen Ukraine's resilience, private companies have extended free services meant to help the military, civilians and the Ukrainian government. For example, NewsWhip Spike gave free access to their platform to monitor Russian disinformation; Bitdefender provided cybersecurity solutions, and Cloudfare offered

16 *Companies Are Getting Out of Russia, Sometimes at a Cost*, https://www.nytimes.com/article/russia-invasion-companies.html

17 B. Luthi, *Visa, Mastercard and American Express Suspend Russian Operations*, https://www.investopedia.com/visa-mastercard-and-american-express-suspend-russia-operations-5221406

18 G. Miranda, *Joining Apple and others, Microsoft stops sales in Russia amid invasion: 'We stand with Ukraine'*, https://eu.usatoday.com/story/tech/2022/03/05/microsoft-suspends-sales-russia-amid-ukraine-invasion/9389460002/

security systems for the protection of Ukrainian organisations' websites[19]. IBM is constantly monitoring the situation in Ukraine and updating the public of possible cyber threats and ways of combating such attacks. Other firms such as ESET have also engaged their researchers in monitoring and sharing information about ongoing malware threats. Amazon supports the Ukrainian government with migration to cloud and securing critical institutional data[20]. Such tools are useful for both combating possible cyberattacks as well as allowing the Ukrainian society to continue to function, even in the midst of war. Other companies provide direct help to people fleeing Ukraine such as free Uber rides at the Polish border and free temporary stays in Airbnb locations[21].

Threat intelligence sharing is another example of a critical service that the private sector has been providing to support Ukraine long before the war started. Prior to the invasion on 24 February 2022, when Microsoft's Threat Intelligence Center detected a malware capable of damaging governmental data, Anne Neuberger, the U.S. Deputy National Security Advisor for Cyber and Emerging Technology, asked the company to pass the information to other countries as a way of preventing the malware from spreading[22]. This was a great example of how public and private sector organisations can work together to combat Russia's malicious activity. Furthermore, the reports published by Microsoft, which describe the trends within the cyber threat landscape, allow the public and other countries to be aware of and build resilience against cyberattacks.

Finally, financial help remains critical to maintaining continued support of Ukraine. Companies such as Facebook, Microsoft, Amazon, and Google have donated $15 million, $25 million, $10 million and over $35 million respectively, in addition to emergency assistance, including food, shelter and psychological aid[23]. Google, for instance, has committed $10 million in donations to organisations providing immediate humanitarian aid as well as a long-term assistance for Ukrainian refugees in Poland[24]. Donations coming from the private sector are undoubtedly playing an important part in the war

19 O. Krakovetskyi, *Free Software Services And Tools for Ukrainians During a War*, https://medium.com/devrain/free-software-services-and-tools-for-ukrainians-during-a-war-c0007f68d939

20 *How Amazon is assisting in Ukraine*, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine

21 D. Avery, *Supporting Ukraine: Over 61,000 People Book Airbnb Stays in Ukraine Just to Help Hosts*, https://www.cnet.com/news/politics/supporting-ukraine-airbnb-and-tech-companies-get-creative/

22 *As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War.*, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

23 *How Tech is Supporting Ukraine*, https://americaninnovators.com/news/how-tech-is-supporting-ukraine/

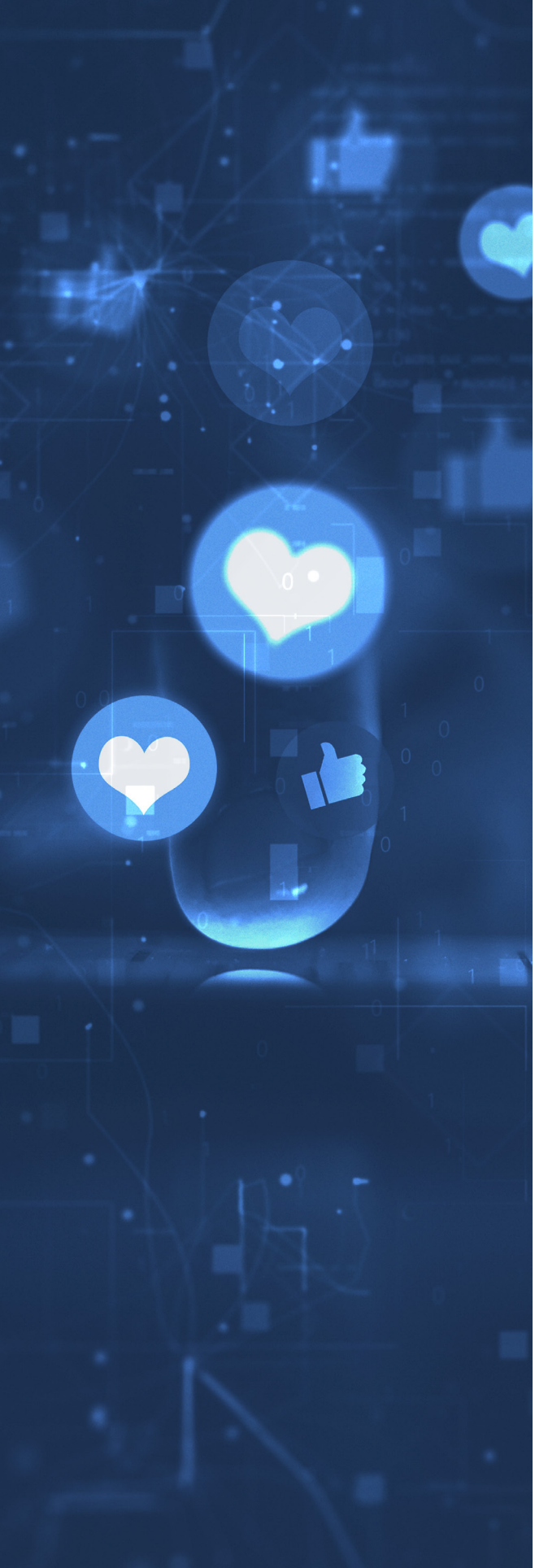
24 Ibidem.

in Ukraine. Whether they are helping the military, the government or the people, they are leaving their mark in this international conflict.

INFORMATION WARFARE AND ONLINE PLATFORMS

Information warfare on the Internet represents a new dimension of a contemporary armed conflict. Russia's efforts to distort reality around the war in Ukraine is a long-standing and organised process that goes back well before the 24 February invasion.

Anti-Ukrainian information manipulation has been deeply embedded in the Kremlin's disinformation efforts for at least 15 years, when the Russians began conducting active influence operations to prepare the ground for the 2014 invasion. In its operations in the information space, Russia emphasises the creation of narratives designed to divide and create distrust, praying on historical and ideological sensitivities, existing prejudices and social conflicts to do so.



SOCIAL MEDIA ACTIVITIES

Ever since the full-scale invasion of Ukraine, social media have played a major role in the conflict. Platforms such as Twitter, Facebook, Instagram, YouTube, TikTok, or even messaging services like Telegram have become a source of information, showing support, but also manipulating the opponent, making information a key puzzle piece to gain advantage in the war. Ukrainian citizens, for instance, have supported their army by using social media platforms to locate the positions of Russian troops (which raises questions about the legal substance of the state of affairs for such actions). Later on they have also utilized the platforms to document and share evidence of war crimes committed by the attackers[25].

Additionally, **leaders such as Mykhailo Fedorov have used social media to pressure private companies into ending their business operations in social media platforms, both in terms of repurposing their main features for information sharing and documenting war crimes, and the amount of new, instant content, the war gained**

25 S. Ankel, *Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up.*, https://www.businessinsider.com/ukraine-hackers-create-fake-profiles-russia-troops-share-location-ft-2022-9?IR=T

a nickname – the 'The TikTok war'.[26]

Russia, on the other hand, utilizes Western social media to spread disinformation as a way to control the narrative of the conflict and discredit claims from Ukraine and its allies. Despite restrictions on the use of social media in Russia, online trolls, fake accounts and bots take state backed disinformation from platforms such as RT and Sputnik and post it on Western social media. The anonymity of the accounts allows them to stay anonymous as they 'merely' repost disinformation. Furthermore, the lack of content monitoring on platforms such as Telegram, which is popular amongst Ukrainians and Russians, allows for disinformation posted there to make its way to Western media through the previously mentioned trolls, accounts and bots.

Due to the accessibility of those platforms, posts from the battlefields allow the public to stay updated in real-time and permit individuals not directly involved in the conflict to quickly spread key information. This becomes a vital tactic for the military when the information which is being spread is in fact disinformation. Research has shown that tweets with disinformation are more likely to be spread than tweets containing the truth.[27] This creates confusion in the public sphere as both sides work towards discrediting the other and fill the media with so much information that it is difficult to recognise the facts. Disinformation is one of the Kremlin's favourite methods to diminish the support for Ukraine and due to its widespread effects, technology companies have started their own battle against this phenomenon.

Since the start of the war, technology companies have begun to restrict their content and block any Russian backed media in an attempt to combat disinformation. Both Twitter and Facebook have blocked accounts spreading false narratives, with the latter also blocking Russian-state sponsored ads and adding warning labels to disinformation posts.[28] Following in the footsteps of Facebook, Google has also prevented Russian state-run news from making money on their platform and restricted some accounts.[29] In its fight against false information, TikTok has been utilizing human monitoring and created a page for digital litera-

26 K. Chayka, *Watching the World's "First TikTok War"*, https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war

27 S. Brown, *MIT Sloan research about social media, misinformation, and elections*, https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections

28 K. Paul, *Flood of Russian misinformation puts tech companies in the hot seat*, https://www.theguardian.com/media/2022/feb/28/facebook-twitter-ukraine-russia-misinformation

29 J. Bursztynsky, *Google, Facebook work to stop spread of Russian anti-Ukraine disinformation with new changes*, https://www.cnbc.com/2022/02/28/google-facebook-battle-to-stop-spread-of-russian-disinformation.html

cy.[30] Independent fact checkers have taken a stand by monitoring posts on social media as well as the Internet, with firms like Google and YouTube sponsoring and teaming up with those organisations.[31] Overall, technology firms have been contributing to the fight against disinformation by both content and account moderation as well as education. It is a difficult task, however, and one among a whole myriad of struggles these companies are faced with.

30 K. Paul, *TikTok was 'just a dancing app'. Then the Ukraine war started*, https://www.theguardian.com/technology/2022/mar/19/tiktok-ukraine-russia-war-disinformation

31 M. Navlakha, *Google and YouTube are investing to fight misinformation*, https://mashable.com/article/google-youtube-fact-checking-misinformation

AREAS FOR IMPROVEMENT

Although propaganda, disinformation and more generally information warfare has been present in social media for many years, the full-scale Russian invasion on 24 February 2022 took the activity in the information domain to a new level. Since then, the largest technology companies have officially declared their support for one of the sides in the military conflict, choosing to stand with the Ukrainian government in the war with Russia. This new reality was a novelty and a challenge for both the users participating in the public debate and for the social media platforms themselves. **The enormous effort involving content moderation, tracking information operations and online manipulation, and navigating the reality of the 'first digital war', with the two parties actively operating in the information space and trying to sway public opinion, meant that the platforms had to put extraordinary measures in place.** In the aftermath of the invasion, Meta, the parent company of Facebook, Instagram, and WhatsApp, reported that it had successfully blocked several Russian accounts that were spreading pro-Kremlin propaganda in Ukraine. A few weeks later, Facebook blocked

access to the regime's Sputnik and RT social media accounts, following action taken at the EU level and by many member states aimed at blocking pro-Russian media outlets. Various experts and representatives of the Ukrainian administration highlight the tardiness of these measures, which were introduced at the behest of the EU, even though these media outlets had been carrying out hostile information activities against Ukraine since at least 2014. The actions of Facebook and Instagram in the context of the Bucha massacre were also a high-profile issue. Immediately after the Russian crimes were revealed, both platforms began blocking, among other things, Ukrainian hashtags and content depicting the effects and scale of the crimes. As Meta's representatives confirmed, these actions were the result of an automated AI system that took them down based on the graphic content they contained, which was said to be in breach of Meta's user terms and conditions. However, the company very quickly restored the content about the Bucha massacre to the platforms, serving as evidence of Russian war crimes.

Despite taking certain measures to combat Russian disinformation activities, Twitter is still widely used to spread Russian propaganda due to a loophole that allows the official Kremlin-related government accounts (mainly embassies from around the world) to spread and amplify disinformation with impunity. While the Kremlin-linked media outlets have started to be labelled as linked to the government of the Russian Federation and the possibility of amplifying content by them has been restricted, Russian embassies continue to enjoy full and unfettered ability to publish and disseminate content that is most often directly Russian and anti-Ukrainian propaganda. They can thus continue to poison foreign information spaces with disinformation.[32]

Content moderation and policy changes which ensue from the battle against disinformation have caused companies to receive a bit of public criticism. While some social media platforms have introduced content moderation as a way of helping Ukraine, civil society and human rights groups have criticized the inconsistency of such policies and insisted on the need to protect users' rights.[33] For instance, critics claim that platforms such as Facebook make content moderation selective rather than universal because in some cases, such as Myanmar, there is little to no content moderation on posts inciting violence whereas in the case of Ukraine content is constantly monitored for disinformation. While public disapproval of decisions made by private compa-

32 J. Clayton, *How Kremlin accounts manipulate Twitter*, https://www.bbc.com/news/technology-60790821
33 S. Biddle, *Facebook's Ukraine-Russia Moderation Rules Prompt Cries of Double Standard*, https://theintercept.com/2022/04/13/facebook-ukraine-russia-moderation-double-standard/

nies is commonplace and does not necessarily make them back pedal, the large amount of disinformation filtering into social media platforms still poses a challenge.

As NewsGuard's research has shown, TikTok is particularly dangerous in this context. According to the study, **a new user of the platform will encounter pro-Russian disinformation after just 40 minutes of use, regardless of their actions: 'TikTok's lack of effective content labelling and moderation, coupled with its skill at pushing users to content that keeps them on the app, have made the platform fertile ground for the spread of disinformation.'**[34] The situation is similar on Telegram, a Russian messaging platform, which is the main tool for communicating and obtaining information in Ukraine, and gaining popularity in other countries such as Poland. Telegram could be described as a safe-haven for creators of alternative content, disinformation, propaganda and conspiracy theories, who benefit from very limited content moderation. What TikTok and Telegram have in common is a lack of meaningful counteraction to Russian disinformation. They also continue to operate in the Russian Federation, responding to the Kremlin's demands (e.g. TikTok temporarily suspended the possibility of livestreaming and uploading new content in Russia in response to a 'fake news' law introduced by the Russian government).[35]

34 A. Cadier, C. Labbe, V. Padovese, et.al., *WarTok: TikTok is feeding war disinformation to new users within minutes – even if they don't search for Ukraine-related content*, https://www.newsguardtech.com/misinformation-monitor/march-2022/

35 R. Bellad, *TikTok suspends content in Russia in response to 'fake news' law*, https://techcrunch.com/2022/03/06/tiktok-suspends-content-in-russia-in-response-to-fake-news-law/

SOCIAL MEDIA IN THE CONTEXT OF GEOPOLITICAL TENSIONS

Facebook and Twitter have been banned from operating in the Russian Federation as a consequence of their actions and a lack of cooperation with the Kremlin. While YouTube continues to operate on the Russian territory, it has restricted the use of advertising, making it impossible for Russian residents to monetise content. At the other end of the spectrum are TikTok and Telegram, which by complying with the Kremlin's demands continue to operate in Russia and remain a source of pro-Russian disinformation beyond its borders. The difference between these two approaches stems from the need to take sides in a geopolitical clash in which the largest social media platforms cannot remain neutral. This is evident in the very examples cited above, which forced some companies to take actions that have the effect of reducing the potential market for their products, limiting their potential profits. While there are still many areas which U.S. technology companies need to work on to combat disinformation more effectively, they are notably simply willing to improve. This is in contrast to platforms such as TikTok from China and Telegram from Russia

which present significant challenges for researchers, experts, policymakers, and decision-makers as they are not fully transparent and it is difficult to fully understand the nature of their operations and the potential impact they may have on disinformation efforts.

COMPANIES AS GEOPOLITICAL PLAYERS

The involvement of private companies in the war was imminent due to the growing tensions in cyberspace in the weeks preceding the outbreak of the war, and also due to the overall character of the conflict which has been taking place both in the physical and cyber domains since the very beginning. **As the 'first shot' of the war was fired in cyberspace, most experts agreed that this conflict would explore the digital frontline in a never-before-seen way.** And they were partially right – the first weeks of the war were marked with countless cyberattacks on the Ukrainian government websites, banking services, and parts of critical infrastructure such as energy plants, with each of those hostile actions against Ukrainian systems making rounds as news from the frontline. Despite the realization a few weeks into the war that the Russian activity in cyberspace was not as damaging as everyone had feared, private sectors companies making up the technological ecosystem knew they had a challenge to meet.

Some of their decisions triggered retaliatory actions from Russia. In the first weeks of the war, Meta started relaxing its content moderation policies on Facebook and Instagram,

allowing speech expressing hatred towards Russia and Russian soldiers. Although Nick Clegg, Head of Global Affairs at Meta explained that the relaxed policy applied only to Ukraine and 'focused on protecting people's rights to speech as an expression of self-defence in reaction to a military invasion of their country'[36], the Kremlin still saw that as a direct attack against its people and therefore decided to ban both Facebook and Instagram across Russia. In a statement by the Russian General Prosecutor's Office, Meta was recognised as an 'extremist organisation' using its platform to incite 'mass riots accompanied by violence'[37] thus, introducing a ban that cost the U.S. company nearly $2 billion in revenue loss.[38]

Companies had surely been aware of the possible risks and potential retaliation. Their decisions – regardless of their magnitude or direction – meant taking an unambiguous stance in the war which due to its technological, digital and cyber aspects will likely go down in history as a geopolitical event of an unprecedented scale. Businesses were dragged into this war, whether they liked it or not, and they stepped up to be the ones changing the course of events.

It is not the first time that the private sector has been tangled up in a military conflict. Besides companies delivering solutions and equipment for the military that was later used in combat, we have seen a few instances of non-military tech businesses finding themselves caught up in armed conflicts (Airbnb and the case of Israeli settlements in West Bank; Facebook and the Rohingya Genocide). Such cases are harsh reminders that although the law does not prohibit companies from operating in conflict-affected areas, their actions can still be deemed political and be prosecuted under local and international laws.

A solution to this might be cooperation with national and international authorities, something that businesses – and governments – have been heavily exercising in the past few years. The public sector's recognition of the immense power held by tech companies initiated a new term in international relations: tech diplomacy. Back in 2017, Denmark was one of the first countries to appoint a tech ambassador to Silicon Valley. In 2022, the European Union also established its 'embassy' in San Francisco, sending Gerard de Graaf to make sure tech companies follow the EU rules

36 Tweet by Nick Clegg, https://twitter.com/nickclegg/status/1502349805221126144?ref_src=twsrc%5Etfw

37 A. Roth, *Russia to block Instagram after Meta relaxes stance on Putin hate speech*, https://www.theguardian.com/world/2022/mar/11/russia-to-block-instagram-after-meta-relaxes-putin-hate-speech

38 A. Brown, *Russia's Instagram, Facebook Bans Will Cost Meta Nearly $2 Billion In Revenue*, https://www.forbes.com/sites/abrambrown/2022/03/11/instagram-facebook-bans-will-cost-meta-nearly-2-billion-in-revenue/?sh=4e3a4bb3262f

while operating on the European market. In the meantime, businesses have also made moves to secure their interests on the international arena – Microsoft established its UN Affairs Office in New York while other tech giants were also negotiating crucial EU policies like the Digital Services Act and Digital Markets Act with the Commission's leaders. We have also seen a few initiatives aimed at setting up rules applying to companies and regulating their activities in cyberspace, such as the 2017 call for a Digital Geneva Convention (ensuring protection of civilians in cyberspace), 2018 Cybersecurity Tech Accord (advancing global cybersecurity), or the 2021 Paris Call for Trust and Security in Cyberspace (promoting multi-stakeholder approach). All those initiatives gained strong support from tech companies, especially Microsoft as one of the leading powers behind these actions. This proves how serious the private sector is about its place in the international system. However, most of the businesses' efforts were made to fulfil the United Nations' Sustainable Development Goals (core of the UN's 2030 Agenda for Sustainable Development focusing on advancing peace and prosperity all around the world) and operating on foreign markets. **War puts a whole new context to their place on the international arena, bringing up a legal dilemma – can private sector businesses be considered participants of the war for their ongoing support of one side or should they be viewed as hapless victims, simply happening to operate on a conflict-affected territory?**

There is a serious risk that companies may be one of the targets of military actions. Based on Microsoft's latest reports, Russia has expanded its cyber activity beyond Ukraine—to Poland, 'a critical logistics hub, in a possible attempt to disrupt the movement of weapons and supplies to the front.'[39] In her Substack post[40], Kim Zetter, a renowned American investigative journalist and author covering cyber and national security issues, argues that the same actions could be taken against cybersecurity companies that support Ukraine and its allies. Citing Mauro Vignati, adviser on warfare technologies to the International Committee of the Red Cross, most networks and systems (even those used by the government and the military) are provided and managed by the private sector, therefore an attack on such infrastructure automatically throws the provider into the warzone. In the event that Russia deemed companies to be involved in hostilities, e.g. by monitoring threats to Ukraine military networks, it could carry out cyberattacks targeting company employees directly. Obviously, such

39 C. Watts, *Preparing for a Russian cyber offensive against Ukraine this winter*, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

40 K. Zetter, *Security Firms Aiding Ukraine During War Could Be Considered Participants in Conflict*, https://zetter.substack.com/p/security-firms-aiding-ukraine-during

an action, if aimed at U.S. businesses specifically, would entail a serious escalation of the conflict between the parties, which would most likely be counter-productive and expose Russia to even greater cyber threats. However, it could become a serious problem during future conflicts in which the U.S. could play an even more significant role, such as a potential Chinese invasion against Taiwan. According to Brad Smith, Microsoft has been 'on the front lines'[41] since the very beginning of the war in Ukraine, especially as Ukraine's government data was moved to the company's cloud infrastructure. And although Russia may not have the right to attack private sector firms providing help to Ukraine, it has shown complete disregard to international laws multiple times.

Ukrainian government does not shy away from acknowledging the private sector's support. President Volodymyr Zelensky introduced a special award – the Ukraine Peace Prize, which was first awarded to Google in May 2022 during the International Economic Forum in Davos.[42] The prize was later given to other tech companies like Microsoft, AWS[43], and Apple. The award is a symbolic recognition

Graphic 2. Mykhailo Fedorov's tweet about the Peace Prize for Microsoft

of the efforts made by those companies to secure Ukraine's infrastructure, systems and networks – efforts which had been discussed and planned in detail during special meetings. Business executives from firms like Apple, Google, Clearview AI held meetings with Ukrainian Minister of Digital Transformation Mykhailo Fedorov and Minister of Defence Oleksii Reznikov, to discuss ways in which they can help the country fight against Russia – and there are three particularly interesting facts about those meetings. One, despite security risks, some of the meetings

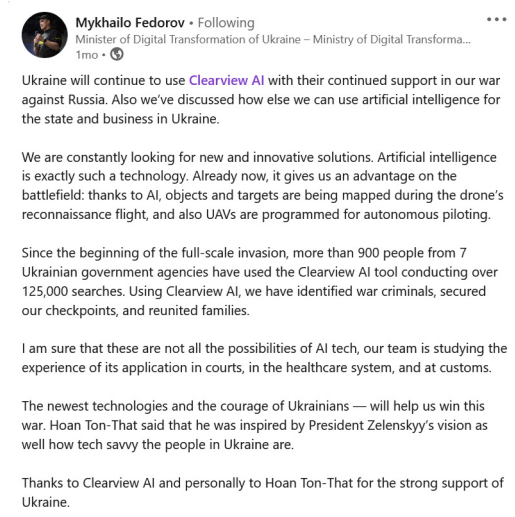
41 Microsoft, *Countering Foreign Information Operations: Developing a whole society approach to build resilience*, via YouTube.com, https://www.youtube.com/watch?v=m_R1jbYoxkI

42 Ministry of Digital Transformation of Ukraine, *Mykhailo Fedorov presented the first Ukraine Peace Prize to Google*, https://www.kmu.gov.ua/en/news/mihajlo-fedorov-vruchiv-pershu-vidznaku-miru-kompaniyi-google

43 B. Nolan, *Zelenskyy awards Amazon the Ukraine peace prize after AWS helped save its 'digital infrastructure'*, https://www.businessinsider.com/zelenskyy-amazon-ukraine-peace-prize-digital-war-support-aws-2022-7?IR=T

were held in Ukraine, during business executives' visits to Kyiv. Two, majority if not all of the meetings were well documented and publicised, both in statements released by the companies or blog posts (e.g., Google's Eric Schmidt's blog post[44]), and also via the official government social media, especially Twitter and LinkedIn accounts belonging to Minister Fedorov. And three, business representatives were treated like equal counterparts during discussions and negotiations. **As conflicts of the past accustomed us to meetings at a presidential, ministerial, or general officer level, this particular war proves how high position companies are holding in the international game. Eric Schmidt even referred to the conflict as the 'first networked war'[45] and it is hard to disagree with that, given the number, frequency and outcomes of such meetings.** As networking can also be done online, Ukraine's government representatives have utilized social media to get to the hearts and pockets of business executives (e.g. the viral Twitter exchange between Minister Fedorov and Elon Musk discussing Starlink services in Ukraine).[46]

Certainly, such actions are not out of place as they make it much easier to discuss areas of cooperation and directly voice ones needs.



Graphic 3. Mykhailo Fedorov's LinkedIn post about cooperation with Clearview AI

However, striking business deals between the public and the private sector had rarely been so openly publicised and praised. The war in Ukraine changed the perspective on the public-private cooperation and we can expect this trend to continue even after the war ends.

Graphic 4. Twitter exchange between Mykhailo Fedorov and Elon Musk

44 E. Schmidt, *The First Networked War: Eric Schmidt's Ukraine Trip Report*, https://scsp222.substack.com/p/the-first-networked-war-eric-schmidts#%C2%A7the-first-networked-war-eric-schmidts-ukraine-trip-report
45 ibidem.
46 Tweets by Mykhailo Fedorov and Elon Musk, https://twitter.com/elonmusk/status/1497701484003213317

DANGERS OF THE NEW INTERNATIONAL PARADIGM

In past conflicts, companies cooperated with governments because they were contracted to provide specific services, just like Ford was asked by the U.S. government to repurpose its assembly lines to build vehicles and aircrafts for the military during World War II. Nowadays, the partnerships between tech firms and Ukraine's government are based mostly on memorandums, which potentially blur the lines between the rules and responsibilities stemming from such cooperation, as they mostly express an intention to work together, and are not coercive in nature. Setting up clear standards and rules of public-private partnerships in times of military conflicts and other crises will surely be one of the biggest national and international security challenges globally, one that may, however, help reduce chances of any wrongs and mishaps happening in the future.

One area of risk may arise from the centralisation of power of tech companies, in which final decisions are often made by a narrow management team or the owner. Importantly, these decisions, which can indirectly influence the course of military actions, do not carry the same level of legal or political accountability as the choices made by tra-

ditional international actors. Nor is there currently an effective mechanism for holding technology companies accountable for the policies they implement. This can be particularly dangerous in the context of state actors treating technology companies as permanent partners for action in the international sphere. After all, business' policies are modified based on the decisions of a single individual or as a consequence of ownership changes. An example of this is the purchase of Twitter by Elon Musk, which quickly resulted in the invalidation of a large part of the platform's previous policies. In extreme situations, this can have negative consequences for activities in the military or the geopolitical domain, as these changes can be drastic, dynamic and happen without any democratically obtained mandate or any appropriate level of accountability. This dependence poses a possible risk to international security, as demonstrated by Musk posting a series of tweets propagating pro-Kremlin ideas, including suggestions of redoing referendums on the occupied Ukrainian territories and formally recognising Crimea as part of Russia.[47] **This raises legitimate questions about a long-term reliability of private sector companies, as national security should not depend on whims and impulses of people who rarely bear any consequences for their actions in war, from the legal standpoint at least.**

When considering the level of involvement of technology companies in international conflicts, a basic fact cannot be overlooked. These companies are private business operations designed primarily to generate revenue. The same applies to U.S. companies which provide services ensuring Ukraine's security. This means that even in the context of an armed conflict, their provision of services requires funding, which may become problematic at some point for the war-torn country and its allies.

An example of this is the unclear situation around the use of the Starlink system in Ukraine. Used to maintain constant communication and information flow for the military and civilian purposes, the technology was initially operating on the Ukrainian territory on the basis of a free subscription provided by the company. However, the subscription was stopped after Elon Musk announced that the company would no longer be able to maintain the service for free and that the cost must be borne by either the U.S. or the Ukrainian government. Furthermore, Musk also made comments about 'donating' the terminals and losing money, when in reality thousands of Starlink kits had been bought and then sent free of charge to Ukraine for example by the Polish government and other companies like Orlen. This highlights the threat of instability of ser-

47 Tweets by Elon Musk, https://twitter.com/elonmusk/status/1576969255031296000

vices provided by the private business, especially in such important and strategic areas.

Finally, cyber activities involve a high level of networking and are cross-border in nature. This creates a risk that the involvement of technology giants in Ukraine may trigger a retaliatory response against their systems, negatively affecting other countries, thus extending the conflict to the cyberspace of countries not involved in the direct fight. In a report published in December 2022, Microsoft warned of potential cyberattacks on 'countries and companies that supply Ukraine with vital aid and weapons supply chains.'[48] This may result in an escalation of hostile cyber activities of a trans-border nature, in which companies involved in providing cyber assistance to Ukraine will be taken as a direct target, and with them their systems and infrastructure stretched across multiple countries and regions. After all, malicious software might spread in an uncontrolled way, much like the NotPetya cyberattacks from 2017 which crossed the Ukrainian border.

48 C. Watts, *Preparing for a Russian cyber offensive against Ukraine this winter,* https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

THE TWILIGHT OF THE NEUTRALITY OF DIGITAL TECHNOLOGY

The war in Ukraine forces us to revisit the myth of technology neutrality and face potential consequences. For decades, technology has been seen as neutral by default – it is the way we use it that adds the value, whether we use it maliciously or to do good. People have the power to dictate the meaning of technology, oftentimes unintentionally, as good intentions can lead to bad outcomes.

This argument is often raised by platforms which claim to be outlets for distributing information without controlling the content and the message behind it. Social media companies have fought for years against governments that tried to enforce onto them responsibility for content inciting violence, spreading hate speech or conspiracy theories. Recent years have shown, however, that the private sector can – and should be taking decisive steps to fight the Kremlin's propaganda off their services, to end up on the right side of history. As Steven Feldstein pointed out in his article for Foreign Policy, the companies 'are now making explicit value judgments regarding how governments use their platforms in wartime and what types of speech violate the bounds

of hate, violence, and propaganda. These actions contradict prior content policies and indicate that companies are hastily rewriting their rulebooks – often in an ad hoc manner – in response to recent events."[49]

As tech firms may not enjoy the privileges of Swiss-like neutrality, their role in international conflicts has to be somehow regulated by international laws. Among other things, both written laws and customary laws must be put in place to define the terms on which such companies may engage in an armed conflict, what responsibilities they will have as a result, and at the same time what prerequisites they have to meet in such a situation. However, bearing in mind that international law is governed more by the principle of consensus than by the coercive enforcement of its rules, and, moreover, that Hi-Tech corporations operate simultaneously in multiple, often disparate legal systems, it is not possible to establish rules regulating every single aspect of the activities of such companies during an armed conflict. The widely known two bodies of law jus in bello and jus ad bellum focus on nations and individuals, not companies; therefore the latter may choose to define and conduct their activity based on cyber norms and initiatives like Cybersecurity Tech Accord[50] which was already signed by some of the biggest tech companies.

Is the myth crumbling before our eyes? Not necessarily. However, it is clear that geopolitical and security events have the power to change the way we use technology, how we think of it, and to what extent we are willing to use digital tools to support our goals. The 'good' version of the myth associated with the belief that the development of new technologies always brings positive consequences for humanity has conclusively collapsed. And as much as modern IT solutions can support human development, they can also serve as a tool for spreading disinformation or carrying out attacks on critical infrastructure supplying society with essential products and services.

Our new reality, where both the public and the private sector cooperate in the technological and security area, cannot be based on the sheer belief in neutrality and good intensions. We need a legal framework to regulate what tech companies can and cannot do in times of international crises, both in the physical and the borderless cyber domain of conflict, especially as the latter is becoming an even bigger part of the modern warfare.

---

49 S. Feldstein, *4 Reasons Why Putin's War Has Changed Big Tech Forever,* https://foreignpolicy.com/2022/03/29/ukraine-war-russia-putin-big-tech-social-media-internet-platforms/

50 Cybersecurity Tech Accord website, https://cybertechaccord.org/

SUMMARY AND RECOMMENDATIONS

Technology companies have played a key role in defending Ukraine from Russia's cyberattacks. Without their participation, it is almost certain that Russia's cyber operations could have tipped the scales of the military action in its favour. Without their ad-hoc changes to content moderation policy, Russian narratives would have flown freely to the West, swaying public opinion and sowing doubt among Ukraine's allies. Despite the unquestionable benefits for the rule of law and fight against unprovoked and violent aggression, this development has serious political and social implications to consider.

As technology companies gain more importance and influence on the international stage, they are becoming key players in the modern geopolitical balance of power. With their powerful financial resources, a network of assets critical for the functioning of the state, and the ability to create public discourse through social media, the top executives of the companies hold in their hands a power that can have direct or indirect influence on the decisions of various stakeholders. These executives are not democratically elected representatives of the public and their accountability lies mainly with their shareholders, so their priorities may not coincide with the sentiments of the general public. Furthermore, their global reach may

make it difficult for international and state legislators to properly regulate and hold them accountable.

The war in Ukraine calls for even stronger public-private cooperation on critical aspects of the functioning of the state. Tech companies' growing importance in the international arena requires the strengthening of international regulations regarding user protection standards, technology and digital infrastructure. Nowadays social media are a major battleground in the information war played out between Russia and the West, and in many other conflicts around the world. Content moderation may therefore become a bone of contention in the relations between the government and the private sector.[51]

However, more defence-oriented countries also have their own tools which are more or less effective in creating High Tech assets. For example, cutting off access to some social media platforms by Russia has led to the emergence of new Russian alternatives like Rossgram which has replaced Instagram. Also the limited availability of Visa and Mastercard online payment methods will likely make Russia switch to China's UnionPay system.

RECOMMENDATIONS FOR POLICYMAKERS:

1. Develop clear guidelines and regulatory frameworks that explicitly define the roles and responsibilities of technology companies during international conflicts, including their obligations, type and scale of permissible aid and conditions under which this assistance can be provided. These regulations need to be developed in close cooperation with the private sector who is already at the forefront of setting norms of responsible behaviour. It is inevitable that such regulations must be created on the basis of a compromise between often contradictory interests of individual countries and corporations, because only the universal character of the rules will make them universally respected. This will probably take place at the expense of detail and unambiguity of these regulations.

2. Ensure ways of communication between tech companies and governments, with open channels for a two-way dialogue, so that assistance may be provided without delay and in a coordinated fashion. Ultimately, however, it is the states, and the international community they create,

51 *Ukraine conflict: Digital and cyber aspects*, https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects

that must have the final, decisive voice in solving the problems arising in the field under discussion.

3. Encourage transparency and accountability to make sure that tech companies adopt responsible practices of behaviour and adhere to the national and international standards and guidelines promoting open Internet model and removing digital barriers.

RECOMMENDATIONS FOR TECH COMPANIES:

1. Clearly communicate your geopolitical agenda, ensure transparency, and state your commitment to the ethical principles such as respect for human rights and free and open Internet;

2. Work closely with international stakeholders to further regulate norms of responsible behaviour in cyberspace and in regard to technology and infrastructure that you are responsible for, as well as coordinate assistance to Ukraine and other countries in need;

3. Engage in an open dialogue with other stakeholders and NGOs to further properly assess your status as geopolitical players and increased influence on global affairs.

CYBERSEC
FORUM / EXPO

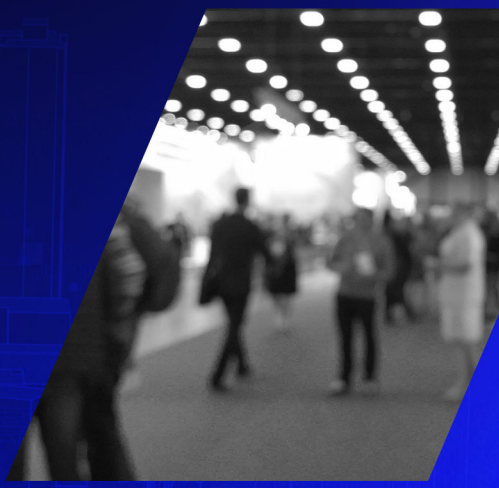
THE KOSCIUSZKO INSTITUTE

#Cyber Made InPoland

/SAVE THE DATE

15-16 JUNE 2023

KATOWICE INTERNATIONAL CONGRESS CENTER




THE KOSCIUSZKO INSTITUTE