Atlantic Council
CYBER STATECRAFT INITIATIVE

Building the digital front line:

Understanding big tech decision-making in Ukraine

Emma Schroeder

Atlantic Council

CYBER STATECRAFT INITIATIVE

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2025

Author

Emma Schroeder

Acknowledgments

This report was made possible by the participation of dozens of scholars and practitioners who shared their expertise and experiences with the author.

Thank you to the Cyber Statecraft Initiative team for their support, particularly Nikita Shah and Trey Herr for their guidance. Particular thanks to Emerson Johnston, Grace Menna, and Zhenwei Gao for their research assistance, as well as to Nancy Messieh, Samia Yakub, and Donald Partyka for the creation and review of language and digital assets. All errors are the author's own.

Table of contents

Executive summary 2

Introduction 3

Pull factors 4
- Clarity of conflict 4
  - *Reaction – Ukrainian tech diplomacy 4*
- Business alignment 6
  - *Reaction – Ukrainian technical capability and posture 9*

Push factors 13
- Difficulty of coordination 13
  - *Reaction – International aid facilitation 14*
- Risk of retaliation 17
  - *Reaction – Risk definition and mitigation 20*

Key takeaways and conclusion 22

About the author 24

Executive Summary

The war in Ukraine has seen Russia launch and sustain a full-scale invasion across the information and physical domains against a country that has embraced technological development and increased technological and geopolitical connections to the United States, Canada, and Europe. Private technology companies have provided essential and often irreplaceable support to Ukraine following Russia's invasion in 2022 and—especially in the early months of the conflict—did so largely without a request from an allied state or payment from Ukraine.

However, more than three years on, although the private sector's assistance in Ukraine has been well-documented, the policymaking community at large is still largely unaware of how companies decided whether and how to provide technological support to and in Ukraine. Through open research as well as interviews and roundtable discussions with various private sector and government representatives, this report posits that companies were primarily motivated by a complex combination of factors in tandem, which pulled them toward or pushed them away from support. The factors pulling companies toward cooperation were the moral clarity of the conflict, and alignment with existing business opportunities. At the same time however, among factors pushing companies away from involvement in Ukraine was the difficulty of coordinating assistance in-country, as well as the risk of Russian retaliation. Meanwhile, both sets of factors were either enhanced—or mitigated—due to various actions taken by Ukraine, allied states, and international bodies. This includes Ukrainian tech diplomacy; the development of Ukraine's technical capabilities; aid facilitations and coordination efforts by both various groups and entities; and risk mitigation efforts undertaken by both states and private companies.

Dependency on the private sector in the cyber domain has become a somewhat frequent refrain in domestic cybersecurity conversations. However, prior to the February 2022 Russian invasion of Ukraine, no one—not supranational bodies, states, or even companies themselves—was prepared for the role they would assume once the tanks rolled and the missiles fired. The Russia-Ukraine conflict's cyber dimension has revealed an underlying dependency on products, services, and infrastructure owned and operated by private companies. This has proved to be both a source of opportunity to enhance Ukraine's defenses, while at the same time revealing fundamental risks and vulnerabilities. Given the heft and impact of technology companies in today's digital infrastructure, let alone in conflict, it is essential that policymakers grasp this complex interplay of factors that influenced companies' decision-making as they headed in Ukraine, to inform planning or preparedness for future conflicts where the private sector will inevitably play a key role.

Introduction

Amid the Russia-Ukraine conflict, the private sector was and is a crucial line of defense and source of cyber resilience to a greater extent than any conflict previously observed. As the first case study of this phenomenon in an overt, conventional war, the past three years in Ukraine have clearly demonstrated how crucial the cyber and informational domain, and the private companies at its forefront, will be in competition, conflict, and war to come.

More than three years following the full-scale Russian invasion of Ukraine in the early morning of February 24, 2022, the war—and the crucial role of the international community in it—continues, but not unchanged. The war that Putin expected to end in Russian victory within a handful of days is now well into the third year of the largest and deadliest war in Europe since World War II.

This study examines the characteristics of this conflict that influenced companies' decision-making regarding the type and degree of their involvement in Ukraine. Which factors and actions taken by states shaped tech companies' decisions throughout the conflict as to whether and how to lend their support to Ukraine? These include both *pull factors*, those that increased the likeliness and degree of technology company involvement in Ukraine, and *push factors*, those that decreased the likeliness or degree of the same. Additionally, a key element influencing this space was the response by the Ukrainian government, allied governments, and international bodies to either build on the effects of the *pull factors* or mitigate the effects of the push factors throughout the conflict.

These factors and reactions are explored through open research, individual interviews with executives from tech companies active in Ukraine,[1] and workshop discussions including private sector, civil society, and representatives from various governments. It puts forward the private sector's perspective on its own involvement in Ukraine since the 2022 invasion, reflecting on opinions and actions as they stood at the time of initial decision but also on the lessons learned since. The intention is to contribute to a baseline of understanding of public-private cooperation in Ukraine so that future policy decisions, whether in the Ukraine context or beyond, are built upon a full evaluation of experience.

Table 1: Push and pull factors

FACTOR	REACTION
Pull	
Clarity of conflict	Ukrainian tech diplomacy
Business alignment	Ukrainian technical capability and posture
Push	
Difficulty of coordination	Ukrainian coordination; Allied government aid facilitation
Risk of retaliation	Risk definition and mitigation

1. All unattributed interviews were conducted in confidentiality with the author, and the names of interviewees are withheld by mutual agreement.

Pull factors

Clarity of conflict

Clarity of conflict refers to the perception of the "right" and "wrong" or "victim" and "perpetrator" in a conflict, among one or more set audiences, whose support has the potential to provide materiel aid. In examining the role of this factor in the provision of tech aid to Ukraine, these audiences are primarily state policymakers, general populations, and technology leaders in Europe and North America. Overwhelmingly, in both public reporting and private interviews, the central reason given by companies themselves for why private companies provide aid and services supporting Ukraine is the moral clarity that these companies, their employees, and a large portion of their customers saw in the conflict and its conduct. Many interviewed commented on how the Russo-Ukrainian War, distinct from most other conflicts, has a clear and binary "right" and "wrong" side in the perspective of at least most of the Western world, from governments to individuals.

Russia engaged in continuous overt and covert aggressive action through a wide variety of coercive, though largely nonescalatory, tools in an attempt to exert control on Ukraine and its population. On February 24, 2022, however, Russia unleashed coordinated missile strikes on Ukrainian cities, airborne deployments of soldiers to key locations beyond the border region, conventional advancement across the border, and coordinated cyber aggression.

In March 2022, Amnesty International released a statement saying, in part, that "In less than a week, Russia's invasion of Ukraine has triggered a massive human rights, humanitarian, and displacement crisis that has the makings of the worst such catastrophe in recent European history."[2] Photos and videos poured out of Ukraine, documenting Russian violence and war crimes against the people of that country. Reports on Russian atrocities and Ukrainian resistance dominated the headlines and news discussions in the West for months. A Monmouth University survey conducted in March 2022 found that 89 percent of Americans believed that Russia's actions in Ukraine were not justified.[3] Similarly, a poll of public perceptions of responsibility for war, taken across ten European countries showed that a clear majority in all countries attribute the primary responsibility to Russia.[4]

During these early months of 2022 the private sector quickly became an essential pillar of support for the Ukrainian war effort. As one expert put it, "If you had ordered a generic villain, you would have gotten Putin. From a moral standpoint, it was really easy for companies to take a stand, you have a moral highpoint."[5] Russia's long decade of slowly escalating violence toward Ukraine, culminating in a brutal conventional assault and now, yearslong war, created an unusually stark geopolitical environment in which both Western states and the majority of their populations not only supported the defense of Ukraine but did so enthusiastically.

Across interviews and roundtable discussions, industry experts demonstrated an appreciation of the clarity of the 'right' and 'wrong' in the case of Ukraine. Nearly every private sector individual interviewed highlighted the importance of this factor in determining whether and how their company decided to begin or deepen its involvement in Ukraine following the invasion. One expert from a leading tech company said that "This was the easiest of all scenarios I could imagine for the private sector to seek to help an entity like Ukraine. The clarity on the conflict made the decision to assist Ukraine clear."[6] As several experts attested, much of the cyber aid provided to Ukraine required technical expertise that was not only limited to a few companies but also limited to a relatively small population of skilled individuals. At this level of analysis, the degree of available assistance had to take into account the bandwidth and possible burnout risk for these individuals as well as a strong, prevalent reluctance to work with a government or, especially, a military. The perceived clarity of the war in Ukraine, however, was critical to overcoming these concerns—at least for a while.[7]

2. "Russia/Ukraine: Invasion of Ukraine Is an Act of Aggression and Human Rights Catastrophe," Amnesty International, March 1, 2022, https://www.amnesty.org/en/latest/news/2022/03/russia-ukraine-invasion-of-ukraine-is-an-act-of-aggression-and-human-rights-catastrophe/.
3. "Majority back U.S. troop presence in Europe, but not in Ukraine itself," Monmouth University Polling Institute, March 16, 2022, https://www.monmouth.edu/polling-institute/reports/monmouthpoll_us_031622/.
4. Catarina Thomson et al., "European public opinion: united in supporting Ukraine, divided on the future of NATO," *International Affairs* 99, no. 6 (2023): 2485–2500, https://doi.org/10.1093/ia/iiad241.
5. Interview with threat intelligence executive at US cybersecurity nonprofit, April 2, 2024.
6. Interview with government affairs executive at US multinational technology corporation, March 26, 2024.
7. Industry executive, IT coalition roundtable, Atlantic Council, February 21, 2024.

Reaction – Ukrainian tech diplomacy

Tech diplomacy is the engagement between state authorities and tech companies, civil society organizations, other states, and multilateral fora to influence the development of both technology itself and the policy that surrounds it.[8] Within the early days of the conflict, members of the Ukrainian government and especially the Minister for Digital Transformation Mykhailo Fedorov, rallied for aid across the technology sector. These calls, and the generally positive reception to them, built on arguments regarding the clarity of the conflict. Although this tech diplomacy has been the project of various Ukrainian officials and offices, both before the 2022 invasion and in the years since, a focus in on Fedorov is illustrative of the Ukrainian approach to cultivating and extracting mutual benefit from relationships with international technology companies.

In 2019, Fedorov was tapped as deputy prime minister and minister of digital transformation and was subsequently named deputy prime minister for innovation, education, science and technology and minister for digital transformation and most recently first deputy prime minister of Ukraine - minister of digital transformation of Ukraine.[9] Fedorov and his team have been adept, according to government affairs executive from a US-based multinational technology corporation, at creating and using "carrots and sticks" to influence company leadership and employees to more favorably view Ukraine and to augment their willingness to contribute to its defense.[10]

Fedorov cultivated a strong social media presence with an audience both within Ukraine and across Europe and North America. He emphasized the importance of social media platforms—using primarily English to connect with an international audience—to bring awareness to the dire situation in Ukraine. He pointed to the social media platform X (formerly Twitter), saying it "has become an efficient tool that we are using to counter Russian military aggression."[11] In efforts like United24, the Ukrainian government's official fundraising platform, which began with Fedorov tweeting the government's crypto wallet addresses with an ask for donations,[12] he saw it not just as a fundraising tool, but as a tool that is "keeping people around the world aware of what is going on in Ukraine."[13] Crowdfunding efforts, even if donations are small, make people feel that their contributions are making a difference and fosters a closer relationship between that person and the Ukraine regardless of the distance.

Fedorov leveraged this engaged global audience to incentivize company action, effectively mobilizing his audience's attention. A look at Fedorov's social media presence shows a clear pattern of this strategy in action. Between March 2022 and July 2024, Fedorov posted fifty-two requests for aid from specific companies, celebrated companies and individuals taking positive action, and called out companies engaging in business practices that he deemed detrimental to Ukrainian defense efforts. These posts served as additional public acknowledgement of the contributions of specific companies to Ukraine in a global public forum that other states were watching, as were individuals, aid organizations, and companies. One tech executive explained that not only did these callouts serve as thanks, they also leveraged the competitive nature of these companies that "one up" each other with aid as an additional driver.[14]

The Starlink case provides an interesting example of this strategy in action. Fedorov tagged Elon Musk in an X post and asked him directly to instruct SpaceX to provide Ukraine with Starlink stations, calling him out for trying to "colonize Mars" instead of helping civilians on Earth.[15] Musk responded publicly on X less than twelve hours later that, "Starlink Service is now active in Ukraine. More terminals en route." Two days later these stations, which would come to serve critical functions for civilians, government entities, and even military personnel, arrived. Fedorov again publicly responded on X with a photo

8. "The TechPlomacy Approach," Ministry of Foreign Affairs of Denmark, accessed October 20, 2025, https://techamb.um.dk/the-techplomacy-approach.
9. "Mykhailo Fedorov," Government Portal (Ukraine), accessed Oct 15, 2025, https://www.kmu.gov.ua/en/profile/mikhaylo-fedorov.
10. Interview with government affairs executive at US multinational technology company, March 26, 2024.
11. Joe Tidy, "Ukraine Crisis: Tech Firms Curb Services in Russia," *BBC News*, March 4, 2022, https://www.bbc.com/news/technology-60608222.
12. Peter Guest, "Mykhailo Fedorov Is Running Ukraine's War Like a Startup," *WIRED*, July 25, 2023, https://www.wired.com/story/ukraine-runs-war-startup/?_sp=f5dd85ca-06aa-46ec-b716-b7cda17ce4f4.1721243250176. Tom Wilson, "Ukraine raises $13 million in crypto after crowdfunding appeal," *Reuters*, February 28, 2022, https://www.reuters.com/world/china/ukraines-government-raises-crypto-worth-8-million-crowdfunding-appeal-2022-02-27/.
13. Guest, "Mykhailo Fedorov is Running."
14. Interview with government affairs executive at US multinational technology corporation, August 28, 2024.
15. Mykhailo Fedorov (@FedorovMykhailo), "@elonmusk, while you try to colonize Mars — Russia try to occupy Ukraine! While your rockets successfully land from space — Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand," X, February 26, 2022, 7:06 a.m., https://twitter.com/FedorovMykhailo/status/1497543633293266944.

of a truck full of terminals saying, "Starlink - here. Thanks, @elonmusk."[16]

According to Fedorov's deputy minister, Alex Bornyakov, in the months leading up to the Russian invasion, Fedorov's office was unable to secure a meeting with Elon Musk. However, SpaceX President and COO Gwynne Shotwell indicated in March of 2022 that the company had been coordinating with Ukraine as part of its European expansion effort for several weeks before the invasion and were awaiting final approval from the Ukrainian government. According to Shotwell, "they tweeted at Elon and so we turned it on … that was our permission. That was the letter from the minister. It was a tweet.[17] These early interactions show that at the very least, Fedorov's social media engagement functioned as a nontraditional method to accelerate the provision and delivery of essential technical equipment that would enable connectivity for civilians, government entities, and even military units.[18]

Six months before the February 2022 invasion, Fedorov went on a tech diplomacy tour to Silicon Valley, intent on building stronger relationships with key technology companies with Ukraine's digital transformation on the agenda. Fedorov's tech diplomacy work laid a solid foundation for coordination between the Ukrainian government and these technology companies by the time the war began. These relationships and Fedorov and his ministry's direct approach with private companies meant that his office could seek solutions in the private sector directly and more swiftly than in traditional government acquisition. For example, in less than a month, a new and improved air raid alert system was implemented across the country as a result of a direct and informal conversation between Ajax Systems Chief Marketing Officer Valentine Hrytsenko, Deputy Minister of Digital Transformation Valeriya Ionan, and a team of digital transformation officers.[19]

Therefore, Ukraine's approach to tech diplomacy represents a significant shift in how states, especially small or mid-power states, should conceptualize and shape their relationships with technology companies. Given that global technology companies' ("big tech") yearly revenue continually overshadows the gross domestic product (GDP) of many states,[20] this evolution in states' relationships with big corporations suggests that corporate ties are sometimes more important than a state's relationship with another state. This was echoed in a statement from the Danish government, recognizing the extent to which technological disruption affects societal and geopolitical change, nothing that the companies driving that innovation "have become extremely influential; to the extent that their economic and political power match—or even surpass—that of our traditional partners, the nation states."[21] Fedorov's actions therefore proved the importance of tech diplomacy as a key government priority to secure the cooperation of the tech sector in a crisis, aided by the moral clarity that many companies saw in assisting Ukraine in a time of war.

Business alignment

For companies examining whether and how to provide tech-based support to Ukraine in its defense, business alignment can take a variety of forms, but typically refers to some combination of benefits that the company receives from these activities. Although the primary driver cited publicly for tech companies' involvement has been the desire to aid Ukraine, their customers, and employees in Ukraine against blatant Russian aggression, another factor in companies' decision-making was in fact how the provision of assistance to Ukraine fit into and supported the overall health and security of their organizations. This included the character of preexisting relationships with both Ukraine and Russia, direct financial profit, and indirect benefits such as instructive experience, field-testing products, and reputational benefits.

16. Elon Musk (@elonmusk), "Starlink service is now active in Ukraine. More terminals en route," X, February 26, 2022, 5:33 p.m., https://twitter.com/elonmusk/status/1497701484003213317; Mykhailo Fedorov (@FedorovMykhailo), "Starlink — here. Thanks, @elonmusk," X, February 28, 2022, 3:19 p.m., https://twitter.com/FedorovMykhailo/status/1498392515262746630?s=20&t=vtC-M9UqgWRkfxfrEHzYTGg.
17. Jeff Foust, "SpaceX Worked for Weeks to Begin Starlink Service in Ukraine," *SpaceNews*, March 3, 2022, https://*SpaceNews*.com/spacex-worked-for-weeks-to-begin-starlink-service-in-ukraine/.
18. Emma Schroeder with Sean Dack, *A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment, Atlantic Council*, February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.
19. Guest, "Mykhailo Fedorov is Running."
20. Alphabet Inc., "Exhibit 99.1 (Q1 2023)," *SEC EDGAR*, April 25, 2023, https://www.sec.gov/Archives/edgar/data/1652044/000165204423000041/googexhibit991q12023.htm; Alphabet Inc., "Exhibit 99.1 (Q2 2023)," *SEC EDGAR*, July 25, 2023, https://www.sec.gov/Archives/edgar/data/1652044/000165204423000067/googexhibit991q22023.htm; Alphabet Inc., "Exhibit 99.1 (Q3 2023)," *SEC EDGAR*, October 24, 2023, https://www.sec.gov/Archives/edgar/data/1652044/000165204423000088/googexhibit991q32023.htm; Alphabet Inc., "Exhibit 99.1 (Q4 2023)," *SEC EDGAR*, January 30, 2024, https://www.sec.gov/Archives/edgar/data/1652044/000165204424000014/googexhibit991q42023.htm; The "GDP (current US$)," World Bank, accessed October 20, 2025, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.
21. "The TechPlomacy Approach."

Preexisting relationships

The Russian invasion of Ukraine in February 2022 was not the start of the conflict between the two nations, nor was it the beginning of technology companies' relationships with Ukraine and Russia. The nature and tone of these relationships provided a key foundation for these companies' decisions throughout the post-2022 conflict. Ukraine and Russia, both as partners and as markets, had different starting points and were also on different active trajectories that informed the types and depth of engagement that tech companies wished to have with each country, both individually and comparatively.

One of the primary motivations cited for company involvement in Ukraine after the Russian invasion was the simple fact that many of these companies were already active in Ukraine to some extent and their leadership felt a responsibility to protect its employees and continue to serve its customers within Ukraine. For example, threat intelligence companies like Mandiant and CrowdStrike had been engaged in Ukraine since at least 2014, actively tracking cyber espionage, influence, and attack operations, while companies like Microsoft and Google were actively building capacity in the country despite Ukraine's prohibitions on cloud services. In 2020, Google opened its second research and development center in Ukraine and Microsoft signed a memorandum of understanding with Ukraine's Ministry of Digital Transformation to include a $500 million investment to build two data centers.[22]

Several private sector and government representatives conveyed in private interviews that one of companies' greatest concerns in the first few weeks of the conflict was the safety of their employees in Ukraine.[23] Many companies set up or contributed to programs intended to help employees leave the country, if they wished, or to provide protection measures for those who remained.[24] Additionally, companies with existing customers in Ukraine saw their mission as largely unchanged, seeking to serve their customers regardless of their location.[25] Companies with these preexisting relationships had more reason to continue or expand their work in the country due to these long-term connections.

By contrast, many of these companies also had preexisting, albeit weaker, ties with and in Russia. According to a 2024 report from the Center for Security and Emerging Technology, however, of the eighteen US tech companies that provided "direct assistance on the battlefield and/or services to maintain critical infrastructure or government functions," none had "significant economic or financial linkages to Russia."[26] While Ukraine had undertaken concerted steps to foster mutually beneficial relationships, Russia had been largely coercive. The Kremlin in the years before the 2022 reinvasion sought to tighten control over the Russian information space and exert influence over international tech companies' activities in Russia. For example, in 2021 Russia passed a law requiring large technology companies with a presence in the Russian market to establish Russian offices registered with the Federal Service for Supervision of Communications, Information Technology, and Mass Media, commonly known as Roskomnadzor, or risk severe punitive measures.[27] Some in the industry viewed the move as an attempt to blackmail tech companies into com-

22. Alexander Query, "Google opens research and development center in Ukraine," *Kyiv Post*, January 15, 2020 https://www.kyivpost.com/post/7682; "Ministry of Digital Transformation of Ukraine and Microsoft to Collaborate in Digital Transformation," Microsoft, October 2, 2020, https://news.microsoft.com/en-cee/2020/10/02/ministry-of-digital-transformation-of-ukraine-and-microsoft-to-collaborate-in-digital-transformation/.
23. Interview with government affairs executive at US multinational technology corporation, March 1, 2024; Interview with government affairs executive at US multinational technology corporation, March 26, 2024; Interview with threat intelligence executive at US multinational technology corporation, April 22, 2024, Interview with government affairs executive at US multinational technology corporation; Interview with information security executives at US intelligence and data analysis software technology corporation, May 8, 2024; Interview with subject matter expert on government cyber aid coordination, June, 17, 2024; Interview with threat intelligence executive at US multinational digital communications technology corporation, July 26, 2024; Interview with information security executive at US multinational technology corporation, August 28, 2024; Industry executive, IT coalition roundtable, Atlantic Council, February 21, 2024.
24. Interview with threat intelligence executive at US multinational digital communications technology corporation, July 26, 2024; Iain Martin, "US and Israeli Tech Companies Evacuate Ukrainian Staff From Possible Frontline," *Forbes*, February 17, 2022, https://www.forbes.com/sites/iainmartin/2022/02/17/usand-israeli-tech-companies-evacuate-ukrainian-staff-from-possible-frontline/; Supantha Mukherjee and Paul Sandle, "Cisco CEO Says Quarter of Staff in Ukraine Have Left," Reuters, March 1, 2022, https://www.reuters.com/business/cisco-ceo-says-quarter-staff-ukraine-have-left-2022-03-01/; "A Message to Team Members on the Conflict in Ukraine," FedEx, March 4, 2022, https://newsroom.fedex.com/newsroom/global-english/a-message-to-team-members-on-the-conflict-in-ukraine.
25. Interview with threat intelligence executive at US cybersecurity nonprofit, April 2, 2024.
26. Sam Bresnick, Ngor Luong, and Kathleen Curlee, *Which Ties Will Bind: Big Tech, Lessons from Ukraine, and Implications for Taiwan, Center for Security and Emerging Technology (Georgetown University)*, February 2024, https://cset.georgetown.edu/publication/which-ties-will-bind/.
27. "Putin signs law forcing foreign social media giants to open Russian offices," *Reuters*, July 1, 2021, https://www.reuters.com/technology/putin-signs-law-forcing-foreign-it-firms-open-offices-russia-2021-07-01/; Human Rights Watch, Russia: Growing Internet Isolation, Control, Censorship, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

plying with Russian censorship.[28] Google was one such target of these coercive measures—in a push to force Google to censor the content available on its platforms within Russia, Russian authorities seized the company's bank accounts. In response, Google's Russian subsidiary declared bankruptcy and ceased all but its free services within Russia.[29]

Amplified by the clarity of conflict discussed above, and Ukrainian tech diplomacy efforts for companies to sever financial ties with Russia and the Russian market, the decision calculus for these companies was less complex than it may have been otherwise.

Not all companies chose to leave the Russian market completely. Despite the coercion that Google faced, the company chose to keep YouTube available in Russia; however, without ads for users in Russia and without the ability to monetize content that would "exploit, dismiss, or condone Russia's war in Ukraine."[30] As discussed previously, many companies decided to continue services in Ukraine out of an obligation to existing customers. Depending on the company and the type of product sold or service provided, this same motivation was seen with respect to Russia as well. One tech executive explained that some of these products and services remained active because they provided a benefit to the Russian public, as opposed to the Russian government. For example, YouTube remained partially active, with restrictions, so that the platform could continue to serve as an alternate source of information for Russians.[31]

Direct profit

For companies, both those with an existing presence in Ukraine and those without, providing technical services in and to Ukraine could also serve more clear-cut business interests. Some were at least partially motivated by direct financial gain like new paid contracts and revenue potential such as additional value generated through the delivery of services and the possibility of positive publicity for the company or their products.

Although much of private companies' work in Ukraine was (or started as) free of charge, many others were acquired in a more traditional contractual manner, with either Ukraine or an allied government footing the bill. Company representatives said in several interviews and roundtables that while they wish to continue their work in the country, as the war continues, they will require financial support to do so.[32]

Indirect benefit

Some of the tech companies active in Ukraine derived value from the very act of providing a service itself, with indirect gains that included instructive experience with Russian cyber operations, the ability to field-test products, and reputational benefits.

For more than a decade, many multinational threat intelligence companies have been tracking Russian cyber aggression in Ukraine as part of their core function. These services helped to drive the development of Ukrainian cyber infrastructure, but it was not solely a charitable effort. It was in these companies own interests to gain the closest possible insights into areas like Ukraine that experience a high degree and sophistication of cyberattacks. As a result, these companies sowed valuable intelligence from their experience, and improved their business offerings across the board. As one executive in threat intelligence at a US cybersecurity nonprofit put it: "for threat intelligence companies, having this depth of access is a gold mine, the details delivered out of Ukraine on Russian tactics, techniques, and procedures (TTPs) are quite amazing."[33]

These benefits are not only limited to threat intelligence companies. Companies that run active platforms used by and in Ukraine, such as cloud platforms, also gained greater direct experience against Russian cyber operations. As one executive put it, "while acting as a shield, [these] companies are collecting vast intelligence that can be used to improve their products and protect all their customers."[34] The experience of defending against Russian activity at that scale and volume served as training of sorts for companies' cybersecurity teams.

Both representatives from private companies and the Ukrainian government cited an additional benefit to working in Ukraine during the current war: it served as a testing ground for technology. As Fedorov stated, Ukraine "is the best test

28. Interview with government affairs executive at US multinational technology corporation, August 28, 2024.
29. "Google's Russian Subsidiary Files Bankruptcy Document," *Reuters*, May 18, 2022, https://www.reuters.com/markets/europe/googles-russian-subsidiary-files-bankruptcy-document-2022-05-18/; "Google's Russian Subsidiary Recognised Bankrupt by Court—RIA," *Reuters*, October 18, 2023, https://www.reuters.com/markets/deals/googles-russian-subsidiary-recognised-bankrupt-by-court-ria-2023-10-18/.
30. "Google Wins UK Injunction over YouTube Block on Russian Broadcasters," *Reuters*, January 22, 2025, https://www.reuters.com/technology/google-wins-uk-injunction-over-youtube-block-russian-broadcasters-2025-01-22/.
31. Interview with executive at US multinational technology corporation, date withheld.
32. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2025.
33. Interview with threat intelligence executive at US cybersecurity nonprofit, May 2, 2024.
34. Interview with business development executive at US information and communications technology corporation, July 18, 2024.

ground for all the newest tech … because here you can test them in real-life conditions."[35] Several company executives privately seconded this notion, saying that alongside their company's desire to do the right thing, their work in Ukraine provided proof of concept for their capabilities.[36] Ukraine also offered a means to demonstrate to potential customers the effectiveness of their offerings. Founding partner of Green Flag Ventures Deborah Fairlamb said at a European defense conference that "no one would even look at a product unless it had 'Tested in Ukraine' stamped on it."[37] During a roundtable conversation, a company executive said that governments were more likely, having seen a company's work in Ukraine, to purchase their products and trust that they are secure.[38]

Finally, companies working actively in Ukraine were also motivated by the benefits to public perception and reputation. Popular support of Ukraine meant that companies' support may have improved their reputation by association. In a TIME article from early 2024, author Vera Bergengruen argued that this reputational concern was part of Palantir's decision calculus for its work in Ukraine, by helping to dispel characterization of the company's work as a tool to support intrusive government surveillance. This would situate Palantir's work in Ukraine among its similar efforts to "shed its reputation as a shadowy data-mining spy contractor."[39] Clearview AI's reputational concerns also likely motivated its assistance to Ukraine. The company was sanctioned multiple times throughout Europe for privacy violations and was lambasted in a 2020 New York Times article for its controversial use by law enforcement and private companies to track people through AI-enabled facial recognition.[40] Nevertheless, the company received an outpouring of positive press following public announcements that Ukraine was using this same AI-enabled facial recognition software to identify Russian soldiers, including deceased soldiers and those suspected of committing war crimes in Ukraine.[41] Whether trying to capitalize on a positive reputation or counter negative perceptions, companies benefit from their association with a cause popular across their customer base.

Reaction – Ukrainian technical capability and posture

In both the buildup to war and the conduct of it, some companies with interest in setting up operations in or with Ukraine were reluctant to do so out of concern regarding Ukraine's ability to act as a capable and trustworthy recipient of goods and services. Executives working in threat intelligence and information security at US-based multinational technology companies have pointed to corruption in Ukraine as a barrier to engagement prior to the invasion and a factor that was carefully considered when deciding how to provide aid in Ukraine.[42] This challenge is openly acknowledged in Ukraine's Anti-Corruption Strategy for 2021-25, which states that "corruption prevalence and distrust in the judiciary are the key obstacles to attracting foreign investment to Ukraine."[43]

To mitigate these factors, Ukraine and its partners have invested heavily over the past decade to take on corruption and build out legal, economic, and technical frameworks to transform Ukraine so as to make it a more appealing target for assistance and cooperation from the public and private sectors. According to Alex Bornyakov, Ukraine's deputy minister of digital transformation, Ukraine's sought to develop "the lar-

35. Vera Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab," *TIME*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.
36. Interview with information security executive at US intelligence and data analysis software technology corporation, May 8, 2024.
37. Bergengruen, "How Tech Giants Turned."
38. Industry Executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.
39. Bergengruen, "How Tech Giants Turned."
40. Robert Hart, "Clearview AI: Controversial Facial-Recognition Firm Fined $33 Million for Illegal Database," *Forbes*, September 3, 2024, https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/; Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
41. Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition during War," *Reuters*, March 13, 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/; Kashmir Hill, "Facial Recognition Goes to War," *New York Times*, April 7, 2022, https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html; Vera Bergengruen, "Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company," *TIME*, November 14, 2023, https://time.com/6334176/ukraine-clearview-ai-russia/; Drew Harwell, "Ukraine is scanning faces of dead Russians, then contacting the mothers," *Washington Post*, April 15, 2022, https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/.
42. Interview with government affairs executive at US multinational digital communications technology corporation, May 2, 2024; Interview with information security executives at US intelligence and data analysis software technology corporation, May 8, 2024.
43. "*Anti-Corruption Strategy for 2021–2025*," National Agency on Corruption Prevention (Ukraine), 2021, https://nazk.gov.ua/en/anti-corruption-strategy/.

gest IT hub in Eastern Europe with the fastest growing GDP, industrial parks, and its own security-focused 'Silicon Valley.'"[44]

Anti-corruption efforts

The Ukrainian government's commitment to anti-corruption efforts has been an important factor for the success of the process, which began well before the buildup of Russian tanks on its border. According to the 2025 Organization for Economic Cooperation and Development (OECD) Integrity and Anti-Corruption Review of Ukraine, since 2013 Ukraine "significantly reformed its anti-corruption framework to fight what were then historically high corruption levels in the country."[45]

Ukraine's public and private IT sectors have long been a breeding ground for software acquisition-related fraud, a scheme in which an individual reports the purchase of a legitimate software license but actually buys a pirated or outdated version of that software and pockets the difference. Before 2014, approximately 80 percent of Ukrainian government and private entities were using network software that had either never been or was no longer supported by the associated software vendor,[46] making Ukraine a difficult and unappealing market for software vendors.

In 2014, anti-corruption activists started the ProZorro project, which over the past decade moved public sector procurement, including that of IT infrastructure, to a central platform built around the tenets of transparency, efficiency, and cross-sector collaboration and competition.[47] According to a report by Dr. Robert Peacock, through the use of ProZorro and other anti-corruption efforts, senior officials at Ukraine's State Special Communications Service estimated that "the share of pirated and unsupported software on the country's networks had dropped from more than 80 percent in 2014 to only 20 percent in 2020."[48]

As the conflict in Ukraine escalated into a full-scale war, Ukraine's anti-corruption efforts became even more urgent and essential. For example, UNITED24, the country's official fundraising platform to fund the Ukrainian war effort that has raised approximately $350 million since the beginning of the war, sends money directly into transparent national accounting systems depending on the choice of the donor, with the leading global accounting firm Deloitte auditing platform.[49] In addition, in the first year of the war Ukrainian President Volodymyr Zelenskyy and his government dismissed several high-ranking government officials based on allegations of corruption. This included two of the top Ukrainian cyber officials after they were accused of participated in corrupt procurement practices. According to the country's National Anti-Corruption Bureau, the accused allegedly embezzled $1.7 million between 2020 and 2022 through fraudulent software acquisition.[50] The Ukrainian government's efforts largely mitigated companies' concerns regarding corruption, and those companies that cited corruption as a barrier to working with Ukraine have since commenced programming previously denied to Ukraine on those grounds.[51]

For a private company to make the decision to invest more heavily in Ukraine, the benefits— financial or otherwise—must outweigh the risks. By addressing corruption within the government, and especially tech-related corruption, the Ukrainian government effectively diminished the weight of this factor in companies' overall decision calculus. Crucially, such efforts take time to implement and yet more time to create meaningful change. Had these anti-corruption programs not

44. Oleksandr Bornyakov, "Why Ukraine is Going All In on Tech to Rebuild Economy," *Fortune*, August 24, 2022, https://fortune.com/2022/08/24/ukraine-going-all-in-tech-rebuild-economy-international-oleksandr-bornyakov/.
45. *Integrity and Anti-Corruption Review of Ukraine*, OECD Public Governance Reviews, OECD Publishing, May 2025, https://doi.org/10.1787/7dbe965b-en.
46. Robert Peacock, *The Impact of Corruption on Cybersecurity: Rethinking National Strategies Across the Global South, Atlantic Council*, July 1, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-impact-of-corruption-on-cybersecurity-rethinking-national-strategies-across-the-global-south/; *Software Management: Security Imperative, Business Opportunity,* Business Software Alliance, June 2018, https://www.bsa.org/files/2019-02/2018_BSA_GSS_Report_en_.pdf.
47. Alona Savishchenko, "How Open Source E-procurement System Prozorro Helps to Sustain Ukrainian Economy," Open Source Observatory, European Commission, November 19, 2024, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/e-procurement-prozorro-support-ukrainian-economy; "EProcurement System ProZorro," Observatory of Public Sector Innovation, https://oecd-opsi.org/innovations/eprocurement-system-prozorro/.
48. Robert Peacock, *The Impact of corruption; Software Management*, Business Software Alliance.
49. "About UNITED24," UNITED24 - The Initiative of the President of Ukraine, accessed October 20, 2025, https://u24.gov.ua/about; Guest, "Mykhailo Fedorov is Running."
50. Daryna Antoniuk, "Two Ukraine Cyber Officials Dismissed amid Embezzlement Probe," *The Record*, November 20, 2023, https://therecord.media/two-ukraine-cyber-officials-dismissed-amid-embezzlement-probe; "Misappropriation of UAH 62 million during the purchase of software: the leadership of the State Special Communications Service is suspected," National Anti-Corruption Bureau of Ukraine, news release (in Ukrainian), November 20, 2023, https://nabu.gov.ua/news/zavolod-nnia-62-mln-grn-pri-zakup-vl-programnogo-zabezpechennia-p-dozriu-t-sia-ker-vnitctvo-derzhspetczviazku/.
51. Interview with government affairs executive at US multinational digital communications technology corporation, May 2, 2024; Interview with information security executives at US intelligence and data analysis software technology corporation, May 8, 2024; Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024.

been well underway before 2022, the question of corruption may have significantly deterred companies from deeper involvement in Ukraine.

Ukraine turns toward tech

Instead of sowing distrust in the idea of cyberspace as a safe space for economic and even government services, the past decade of Russian aggression against Ukraine in cyberspace motivated Ukraine to invest heavily in that space and turn its former weakness into a newfound strength. It could even be said that the continuous Russian aggression against Ukraine, through cyberspace and otherwise, helped Ukraine to better defend itself against Russia. Before the 2022 Russian invasion and even more so since, the Ukrainian government sees a flourishing technology sector within Ukraine as a key component to the economic strength of the country.[52] However, to foster such a flourishing tech environment, Ukraine needed to first invest in its legal and economic foundations.

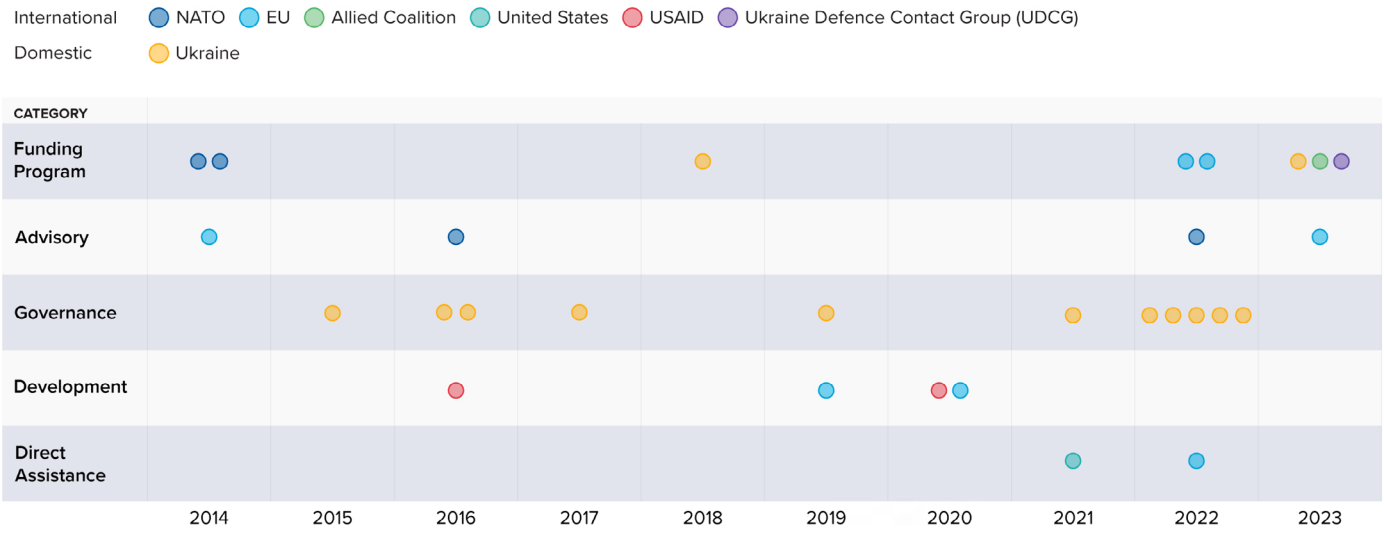
As a response to escalating Russian aggression in 2014, Ukraine began what would be an intensive decade of government reform and policy advancement on cyber issues. The figure below highlights various investment and development programs aimed at enhancing Ukrainian technological capacity, including efforts of the Ukrainian government itself and in partnership with various international entities such as the North Atlantic Treaty Organization (NATO) and the US Agency for International Development (USAID).

These, among other efforts, were essential steps to creating and expanding a technologically capable and developed Ukraine. Especially important was the increased relative cybersecurity of the Ukrainian digital environment, the development of Ukraine's cyber workforce and general cyber literacy, and an influx of capital enabling increased investment in private sector tools and services.

On the economic front, the Ukrainian government made strides to create an attractive environment for investment. The government's mission has been to shift the conversation from purely one of donations and aid to a direct appeal to the companies' more pecuniary concerns. According to Bornyakov, "The best way to help Ukraine is to invest in Ukraine."[53] This call is both international and domestic. The Ukrainian government has implemented a number of projects and programs dedicated to fostering the local tech ecosystem. As of December 2024, the IT sector accounted for 4.4 percent of Ukraine's GDP and 38 percent of the country's total service exports. Much of this technological energy is being dedicated back to the war effort—according to a report compiled in cooperation with the Ministry of Digital Transformation of Ukraine, 97 percent of Ukrainian IT companies are "actively supporting projects that contribute" to Ukrainian defense.[54]

Diia City in particular, launched just two weeks before the invasion, is a tool intentionally designed to make it easier and more appealing for foreign companies to set up and run operations within Ukraine. Diia City is a "virtual free economic zone for

Fig. 1: Development programs aimed at enhancing Ukrainian technological capacity, 2014-2023 select examples



Source: Author

52. Bergengruen, "How Tech Giants Turned."
53. Bergengruen, "How Tech Giants Turned."
54. "Ukrainian Tech Industry Shows Resilience in the Face of War — IT Research Ukraine 2024," *techukraine.org*, December 5, 2024, https://techukraine.org/2024/12/05/ukrainian-tech-industry-shows-resilience-in-the-face-of-war-it-research-ukraine-2024/.

tech companies in Ukraine" that offers a variety of legal and tax benefits.[55] The connected Brave1 initiative launched in early 2023 to "create a fast track for innovation in the defense and security sectors," especially those projects of high importance to Ukrainian military leadership, such as "drones, robotic systems, electronic warfare, artificial intelligence tools, cybersecurity, communications, and information security management systems."[56]

These efforts, both domestic and international, bolstered the defense of Ukraine by building and demonstrating trustworthiness, capability, and economic value for the private sector. In other words, the political and economic engine driving technological development in Ukraine was composed of more than a decade of concentrated action from Ukraine and its international partners, and was in place well before tanks began rolling across the borders. This vital work ultimately helped to bring about conducive conditions for private sector investment or provision of services, as long-term structural factors indirectly shaping company decision-making to aid Ukraine.

55. "Diia City," Diia, accessed October 20, 2025, https://city.diia.gov.ua/en.

56. Mykhailo Fedorov, "Ukraine's Vibrant Tech Ecosystem Is a Secret Weapon in the War with Russia," *UkraineAlert* (Atlantic Council), August 17, 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-vibrant-tech-ecosystem-is-a-secret-weapon-in-the-war-with-russia/.

Push factors

Difficulty of coordination

Difficulty of coordination refers to the friction that private companies experienced along the lifecycle of technical assistance to Ukraine—from understanding which products or services would be impactful, knowing who to coordinate with and how, or the logistics of providing that assistance. Friction, as in all domains of warfare, is the imposition of the constraints of reality upon one's plans and impulses, and therefore each additional complexity that stands between a certain technology and its use in Ukraine increases the likelihood that that desired provision will not occur, will take longer, or will be provided in a less helpful form.

One of the most persistent hindrances to the provision of tech-related assistance from private companies in Ukraine was the difficulties that all parties involved faced, which was to effectively coordinate the assistance available with the assistance that Ukraine needed most in a fast-moving and high-pressure environment, particular as more Ukrainian organizations expressed a need for more threat intelligence, licenses, or training for tools. In almost every conversation with industry representatives about their experience in this space raised this coordination problem. The factors that most significantly impacted coordination effectiveness included whether a company had a preexisting presence in or relationship with Ukraine, the clarity with which Ukraine communicated its technical needs, and the ability to assess the effectiveness and impact of products or services provided.[57]

Especially in the early months of the full-scale Russian war, much of the assistance that private tech companies provided was coordinated by companies themselves and in a largely ad hoc manner. In addition, Ukraine experienced communications challenges such as a lack of secure channels or limited visibility into networks and infrastructure on the ground.[58] Companies that did not have a strong relationship with the Ukrainian public sector prior to the conflict found that direct coordination was difficult to establish once the conflict had begun.[59] For some, not having a direct relationship with or in Ukraine had been an intentional choice, due to regulation complexity or corruption concerns.[60] Initially, companies without a preexisting presence often struggled to pinpoint the correct office or person with which to speak. They bridged this gap most often with some combination of brand recognition driving direct outreach from the Ukrainian government and facilitation by Ukrainian private companies that had established relationships with international tech companies and could act as middlemen.[61]

Even in cases of existing relationships within Ukraine, complexities abound for companies. A threat intel executive indicated that, for many, there is a tension between what companies thought they could provide and what the Ukrainian government knew about its own needs. While Ukraine was effective in communicating its technical needs at the tactical level, according to various company representatives, effective coordination was somewhat hampered by their ability to effectively communicate and coordinate technical assistance needs across government at a strategic level lagged behind.[62]

An additional point of friction was the high degree of difficulty in deconflicting the assistance provided to Ukraine from different companies. Understandably, the Ukrainian government—and various individuals and agencies working within it—were responding to imminent threats and thus would send out the same or similar requests to various companies in the hope that one would respond.[63] This meant that at times various companies were devoting time and resources to developing an assistance measure that was not actually needed and would not be implemented, or if it was in part, had a lesser relative impact on Ukrainian defense because of duplicative measures. This inability to understand and plan around the impact of assistance was broader than just the duplication issue; dozens of company representatives reported difficulties in getting a

57. Greg Rattray, Geoff Brown, and Robert Taj Moore, The Cyber Defense Assistance Imperative: Lessons from Ukraine, Aspen Digital, May 2025, https://www.aspeninstitute.org/wp-content/uploads/2025/05/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf.
58. "CDAC: "The Scale of What We Can Do is Severely Hampered by not Having Funding for Dedicated Staff or to Fulfill Requirements Directly," Common Good Cyber, May 29, 2025, https://commongoodcyber.org/news/interview-cdac-funding/.
59. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024.
60. Interview with business development executive at US information and communications technology corporation, July 18, 2024; Interview with government affairs executive at US multinational digital communications technology corporation, May 2, 2024; Interview with information security executives at US intelligence and data analysis software technology corporation, May 8, 2024.
61. Interview with business development executive at US information and communications technology corporation, July 18, 2024.
62. Interview with threat intelligence executive at US cybersecurity nonprofit, April 2, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.
63. Industry executive, "IT Coalition" Roundtable, Atlantic Council, February 21, 2024.

clear view as to whether their assistance was actually effective once provided.[64]

Without this data, future requests for and fulfillments of technical aid will continue to be based on theory rather than evidence from their growing experiences together. A 2024 paper from the Cyber Defense Assistance Collaborative (CDAC) and Columbia School of International and Public Affairs, made strides in its effort to collate and assess the effectiveness of those companies and organizations that provided cyber defense assistance to Ukraine through their program. The report identified both direct indicators, where effectiveness can be assessed via concrete measures, and proxy indicators, where possible contributing factors are assessed on a scale of perceived impact.[65]

Reaction – Ukrainian coordination and adaptation

On top of domestic development efforts, Ukrainian government officials spent concerted time and effort to build relationships that would serve as the foundation for future cooperation. Fedorov's tech diplomacy work forged new connections with these companies, as well as their leadership and employee bases, that in many ways enabled the speed of company response following Russia's February 2024 invasion. "When the invasion began, we had personal connections to these companies," Fedorov said. "They knew who we are, what we look like, what our values are and our mission is."[66]

According to Fedorov, in the first month of the war he sent "more than 4,000 requests to companies, governments, and other organizations, each one personally signed."[67] Some of these connections built on existing relationships, but companies without preestablished links either initiated conversations directly with or received direct requests from the Ukrainian Government. Beyond the Ministry of Digital Transformation, various Ukrainian offices like the State Special Communications Service of Ukraine, Security Service of Ukraine, National Security and Defense Council of Ukraine, and Ukrainian National Cybersecurity Coordination Center were engaging in relationship building and outreach efforts in order to coordinate the provision of tech assistance.[68] According to Bornyakov, the early days of coordination with the international private sector were chaos.[69] Various offices and employees sent out messages and requests without internal coordination, and products or services were provided without sufficient due diligence to ensure that they were truly useful to the Ukrainian war effort.

The Ukrainian government quickly updated its practices to facilitate more efficient cooperation. Among the first of these moves was a Ukrainian policy change to directly enable increased private sector participation. In February 2022, prior to the invasion, the Ukrainian parliament Verkhovna Rada amended the laws that had barred government use of Cloud services. This change meant that just days before the Russian invasion, companies including Amazon, Microsoft, Google, and Cloudflare were able the aid the Ukrainian government and several critical sector entities in migrating their critical data to their cloud servers—a critical move, as Russia's attacks during the first few weeks of the war specifically targeted physical data centers.[70] In addition, due to the imposition of martial law, Ukraine adopted two resolutions to streamline public procurement. Resolution 169, adopted on February 28, 2022, enabled government contracting authorities to ignore, when necessary, the procurement procedures required by the laws on public and defense procurement.[71] Resolution 723, passed four months later, added new, more efficient requirements to the procurement process, amending both resolution 169 and resolution 822, most important of which was the introduction of the ProZorro platform as the mandatory electronic procurement system.[72] As previously discussed, this platform was both a tool to facilitate procurement and to counter corruption in the procurement process at large.

Despite improvements to coordinate more effectively with private tech companies, and even as international coordination mechanisms emerged, a significant contingent of companies has maintained a preference for direct coordination. One

64. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

65. "Cyber Defense Assistance Evaluation Framework," Cyber Defense Assistance Collaborative, June 18, 2024, https://crdfglobal-cdac.org/cda-evaluation-framework/.

66. Peter Guest, "Mykhailo Fedorov is Running," *WIRED*, July 25, 2023, https://www.wired.com/story/ukraine-runs-war-startup/.

67. Cat Zakrzewski, "4,000 letters and four hours of sleep: Ukrainian leader wages digital war," *Washington Post*, March 30, 2022, https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/.

68. Interview with tech assistance coordination executive, US nonprofit organization, July 17, 2025.

69. Bergengruen, "How Tech Giants Turned."

70. Colin Demarest, "Data Centers Are Physical and Digital Targets, Says Pentagon's Eoyang," *C4ISRNET*, November 17, 2022, https://www.c4isrnet.com/cyber/2022/11/17/data-centers-are-physical-and-digital-targets-says-pentagons-eoyang/.

71. Oleh Ivanov, "Procurement During the Full-Scale War," Vox Ukraine, October 14, 2022, https://voxukraine.org/en/procurement-during-the-full-scale-war.

72. "On Amendments to the Resolutions of the Cabinet of Ministers of Ukraine No. 822 of September 14, 2020 and No.169 of February 28, 2022," Verkhovna Rada of Ukraine, June 24, 2022, https://zakon.rada.gov.ua/laws/show/723-2022-%D0%BF#n2.

government affairs executive noted that their company, like many others, preferred direct coordination with the Ukrainian government since it enabled more immediate and relevant support, and they were skeptical that third-party mechanisms would be as effective.[73]

Reaction – International aid facilitation

Since the February 2022 Russian invasion of Ukraine, and even before that, international entities—states, supranational bodies, and non-state groups— played an important role in coordinating technical-focused aid in support of Ukraine.

However, states' coordination efforts were notably inconsistent. In the first year and a half after the Russian reinvasion, the United States allocated $113 billion in response to the war in Ukraine—largely allocated to the Department of Defense at 54.7 percent, USAID at 32.3 percent, and the Department of State at 8.8 percent.[74] This money should not be viewed like a check signed over to the Ukrainian government, but rather as money allocated to respond to the Russian invasion through a combination of forms and recipients, primarily the defense industrial base in the United States.[75] By contrast, private companies publicly announced and celebrated their digital and tech aid to Ukraine. In an interview, one leading tech executive observed a clear dearth of focus from the US government toward digital and tech aid, instead opting for significant humanitarian and more traditional military assistance.[76] This prioritization was likely an intentional choice—the US government's perspective seems to have been that it was leading conventional aid by a significant margin and wanted others, like European governments and the private sector, to take the lead on digital and tech matters.[77] Though not speaking specifically on cyber and tech elements, Secretary of Defense Pete Hegseth in February 2025 called publicly for European states to provide the "overwhelming" majority of defense funding for Ukraine, bemoaning what he saw as an "imbalanced relationship."[78] Hegseth specifically pushed for the expansion of existing Europe-led coalitions—discussed below—dedicated to coordinating technological aid.[79]

By contrast, industry experts agreed that the UK Foreign, Commonwealth and Development Office (FCDO) was a very effective facilitator of private sector aid.[80] The UK's efficiency on this issue was due in part to fewer restrictions on aid money between distinct civilian- and military-designated buckets.[81] According to an assessment from the Independent Commission for Aid Impact, which scrutinizes UK aid spending, this flexibility enabled the FCDO to respond and adapt to the constant evolutions of the war and geopolitical environment—thereby acting as an effective channel for private sector assistance into Ukraine.[82]

The ad hoc nature of many of the early digital assistance programs provided by private companies was in some ways a double-edged sword. In many cases they were present and able to move more quickly than government programs, and in some places they stepped into de facto political roles—shaping the conflict and public understanding of it. However, this efficiency and effectiveness became difficult to sustain in the long run as governments and government-sponsored mechanisms were slow or insufficient to step in to support these ef-

73. Interview with government affairs executive at US multinational technology corporation, August 28, 2024.
74. Elizabeth Hoffman, Jaehyun Han, and Shivani Vakharia, *Past, Present, and Future of US Assistance to Ukraine: A Deep Dive into the Data, Center for Strategic and International Studies (CSIS)*, September 26, 2023, https://www.csis.org/analysis/past-present-and-future-us-assistance-ukraine-deep-dive-data.
75. The difficulty, for the purposes of this paper, is understanding the breakdown of this assistance as it applies to digital and tech-focused aid to Ukraine. The author found examples breaking down US government assistance by general category (i.e., humanitarian, military, financial) and breakdowns of weapons systems aid (e.g., tanks and air defense systems) but little enumeration of the kind and amount of digital and tech aid provided by the US government. See "Ukraine Support Tracker," Kiel Institute for the World Economy, updated October 14, 2025, https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker.
76. Interview with government affairs executive at US multinational technology corporation, August 28, 2024.
77. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024; Interview with information security executive at US multinational technology corporation, August 28, 2024; Interview with threat intelligence executive and government affairs executive at US multinational digital communications technology corporation, October 2, 2024.
78. Alex Therrien and Frank Gardner, "Hegseth Sets Out Hard Line on European Defense and NATO," *BBC News*, February 12, 2025, https://www.bbc.com/news/articles/cy0pz3er37jo.
79. Jon Harper, "Hegseth Puts Onus on Allies to Provide 'Overwhelming Share' of Weapons to Ukraine," *DefenseScoop*, February 12, 2025, https://defensescoop.com/2025/02/12/hegseth-ukraine-defense-contact-group-allies-military-aid-trump/.
80. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024; Interview with threat intelligence executive and government affairs executive at US multinational digital communications technology corporation, October 2, 2024.
81. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.
82. "UK aid to Ukraine," Independent Commission for Aid Impact (ICAI), April 30, 2024, https://icai.independent.gov.uk/html-version/uk-aid-to-ukraine-2/.

forts.[83] US government entities were instrumental in facilitating support from private companies to Ukraine through purchase agreements, such as that of hundreds of Starlink devices and subscriptions in coordination with other governments[84] and partnerships. US government entities also participated in intelligence sharing and collaboration efforts regarding Russian cyber capabilities and activities[85] and even conducted hunt forward operations to assist in Ukrainian defense against Russian cyber aggression both before and after the February 2022 Russian invasion.[86]

In various conversations, both industry and government representatives confirmed the lack of effective governmental and supranational coordination and its impact on the private sector, and on Ukrainian defense.[87] Company representatives across the United States and Europe shared the same refrain: "we can't keep supporting Ukraine ourselves forever without government assistance."[88]

In addition to bilateral assistance efforts, various entities emerged across the conflict focused on cooperation organization and facilitation of digital and tech aid. The first of these was the CDAC, not a government entity, but a nonprofit organization that brought together a number of cybersecurity and technology organizations to better coordinate assistance efforts. The organization was founded by Gregory Rattray and a coalition of cyber executives to address the impediments and complications that accompanied the early days of digital and tech assistance provision from the private sector. A CDAC representative said in May 2024 that the group had facilitated $20-30 million in tech-related assistance for Ukraine since its inception.[89] As Ukrainian and CDAC representatives noted, CDAC's facilitation efforts have since slowed for a variety of reasons: decreased ability to act as an intermediary as requests have become more specific, a stabilization among companies that no longer require a coordinator after their relationships in Ukraine were established, and a lack of sufficient financial support for both CDAC and the companies willing to provide assistance.[90]

The vacuum noted by industry representatives and CDAC founders in the shape of a true digital and tech aid coordination body with the resources and remit to execute that mission is the planned role of the IT Coalition and the Tallinn mechanism. The IT Coalition, part of the Ukraine Defense Contact Group (UDCG; also known as the Ramstein Group), was established in September 2023 as "a dedicated group of donor nations led by Estonia and Luxembourg within the UDCG framework, focused on delivering support to Ukraine's Defense Forces in the area of IT, communications, and cyber security."91 The group consists of eighteen member countries,

83. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024.

84. "SpaceX, USAID Deliver 5,000 Satellite Internet Terminals to Ukraine," *Reuters*, April 6, 2022, https://www.reuters.com/technology/spacex-usaid-deliver-5000-satellite-internet-terminals-ukraine-2022-04-06/; Alex Marquardt, "Exclusive: Musk's SpaceX Says it Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick Up the Tab," *CNN*, October 13, 2022, https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine; Michael Sheetz, "Pentagon Awards SpaceX with Ukraine Contract for Starlink Satellite Internet," *CNBC*, June 1, 2023, https://www.cnbc.com/2023/06/01/pentagon-awards-spacex-with-ukraine-contract-for-starlink-satellite-internet.html.

85. "United States and Ukraine Expand Cooperation on Cybersecurity," *Cybersecurity and Infrastructure Security Agency*, July 27, 2022, https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity; David Jones, "White House Warns of US of Possible Russian Cyberattack Linked to Ukraine Invasion," *Cybersecurity Dive*, March 22, 2022, https://www.cybersecuritydive.com/news/white-house-warns-russian-cyberattack-ukraine/620755/; Egle Murauskaite, "U.S. Assistance to Ukraine in the Information Space: Intelligence, Cyber, and Signaling," *Asymmetric Threats Analysis Center (University of Maryland)*, February 2023, https://www.start.umd.edu/publication/us-assistance-ukraine-information-space-intelligence-cyber-and-signaling.

86. Maj. Sharon Rollins, "Defensive Cyber Warfare: Lessons from Inside Ukraine," *US Naval Institute Proceedings*, June 2023, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine; "Before the Invasion: Hunt Forward Operations in Ukraine," *US Cyber Command (declassified briefing)*, November 28, 2022, https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf; Dina Temple-Raston, Sean Powers, and

    Daryna Antoniuk, "Ukraine Hunt Forward Teams," *The Record*, October 18, 2023, https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command.

87. Interview with tech assistance coordination executive at US nonprofit organization, July 17, 2025; Interview with government affairs executive at US multinational technology corporation, August 28, 2024.

88. Interview with threat intelligence executive at US multinational technology corporation, April 22, 2024; Industry executive, "IT Coalition" Roundtable, Atlantic Council, February 21, 2024; Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024; Interview with threat intelligence executive and government affairs executive at US multinational digital communications technology corporation, October 2, 2024.

89. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024.

90. Industry executive, "Public-Private Cyber Support" Workshop, Royal United Services Institute, May 29, 2024.

91. "Luxembourg, Estonia, and Ukraine Have Launched the IT Coalition," Government of Luxembourg, September 19, 2023, https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2023/09-septembre/19-bausch-itcoalition.html.

with the European Union, NATO, the United States, and France acting as observers.[92] In 2024 and 2025, the coalition had raised "€1,1 billion in both financial and material assistance."[93] The coalition aims to support Ukraine cyber defense capability and command and control integration while also delivering on more long-term goals such as fostering innovation and cloud adoption. The United States is currently an observing member of the IT Coalition and have thus far has declined taking a more active role. Those familiar with the inner workings of the mechanism have emphasized the clear benefit of a more active US role in the mechanism, as most of the tech companies with whom the organization would like to coordinate are headquartered out of the United States.[94]

The Tallinn Mechanism was established in December 2023 with 11 states to "coordinate and facilitate civilian cyber capacity building" within Ukraine, and is intended to be complementary to military-focused cyber aid facilitation bodies like the IT Coalition.[95] The Tallinn Mechanism is focused on "amplifying the cyber support of donors to Ukraine in the civilian domain."[96] The mechanism raised approximately $210 million by the end of 2024 and has focused on bolstering cyber defense capabilities, especially that of critical national infrastructure, through the public and private provision of hardware and software, incident response, satellite communication provision, and cybersecurity training for government officials.[97]

The international community has certainly made strides to better facilitate technology aid to Ukraine, to counteract the pushing effect that complicates such coordination for technology companies. However, it is yet unclear whether these programs and practices will meet the demands of this conflict, or those of conflicts to come. The most effective element of the tech sector at large's efforts in Ukraine has been its speed, both in its response to the invasion itself and to individual challenges that have arisen over the course of this war. Meanwhile, government and supranational coordination—aside from those programs already in place—were much slower to implement.

Risk of retaliation

A significant factor shaping the behavior of companies' work in and with Ukraine is the heightened threat state created by active warfare. Various technology company officials cited their concern about potential backlash—whether financial, cyber, or physical violence—from Russia against their infrastructure, products, and people.[98] The real risk that these companies took on was informed by a number of factors, such as the application of their products or services by and for military ends, the required physical presence of personnel, products, or infrastructure, and also the degree to which increased Russian aggression against these companies might be a meaningful increase from prewar conditions.

Defense application

An undeniable yet complex risk that companies face as a result of providing support to Ukraine is the threat of Russian retaliatory action. Private sector behavior in Ukraine is shaped by the degree to which the goods and services provided are connected to the conduct of the conflict itself. Products and services provided to civilian groups for purely humanitarian purposes come with a different risk profile than goods that underpin government functions. Though not discrete or exhaustive, cyber and technical aid to Ukraine can be understood in four categories: humanitarian aid, critical infrastructure protection, government support, and military application. In practice, this division exists on a continuum, from purely humanitarian support to products or services that the state itself has come to rely on for the continued provision of government services,

92. "Ukraine Defence Contact Group: Estonia and Luxembourg Announce New Contributions to IT Coalition," *European Pravda*, April 8, 2024, https://www.eurointegration.com.ua/eng/news/2024/04/8/7183316/; "IT Coalition Established by Estonia and Luxembourg ... Has Raised about 500 Million Euros in Its First Year," Republic of Estonia Ministry of Defense, December 12, 2024, https://www.kaitseministeerium.ee/en/news/it-coalition-established-estonia-and-luxembourg-help-ukraine-has-raised-about-500-million-euros.

93. "IT Coalition Led by Estonia and Luxembourg Has Raised over One Billion Euros to Support Ukraine," Republic of Estonia Ministry of Defense, May 28, 2025, https://kaitseministeerium.ee/en/news/it-coalition-led-estonia-and-luxembourg-has-raised-over-one-billion-euros-support-ukraine.

94. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

95. "Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine," US Department of State (Office of the Spokesperson), December 20, 2023, https://2021-2025.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/.

96. "Tallinn Mechanism Raises €200 Million to Support Ukraine's Resilience in Cyberspace," Republic of Estonia Ministry of Foreign Affairs, December 20, 2024, https://www.vm.ee/en/news/tallinn-mechanism-raises-eu200-million-support-ukraines-resilience-cyberspace.

97. "Joint Statement Marking the First Anniversary of the Tallinn Mechanism," US Department of State (Office of the Spokesperson), December 20, 2024, https://2021-2025.state.gov/joint-statement-marking-the-first-anniversary-of-the-tallinn-mechanism/.

98. Interview with government affairs executive at US multinational technology corporation, August 28, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

with particular importance placed on whether the good is for military use and whether that use is in direct support of combat operations.

By and large, companies have made their own determinations as to how to amend their work in Ukraine, looking not only at the direct military application of their product or service but also examining existing and potential products or services to determine potential applicability for offensive operations—and where to avoid their abuse. A clear example of this is Google's cessation of the live traffic display functionality within Google Maps. A team of open source researchers at the Middlebury Institute of International Studies, under the leadership of Professor Jeffrey Lewis, were allegedly able to infer the early movements of the February 2022 Russian invasion before official reporting by analyzing Google Maps traffic data in combination with radar imagery.[99] Following these reports, Google announced that it would temporarily disable live traffic data so that it would not be used to plan military operations.[100] An internal task force at Google largely coordinated these and similar decisions to coordinate aid to Ukraine and, most importantly, to examine their actions and decisions in order to identify and address programs that had a potential to cause harm.[101] However, even after these amendments were made, Google Maps was again the subject of controversy. In November 2024, Ukrainian defense chiefs accused Google of revealing the location of key military positions following an earlier Google Maps update. According to Russian military bloggers, among these revelations was the position of new air defense systems, including US-made Patriot anti-aircraft missiles, surrounding an airport near Kyiv. According to the head of Ukraine's counter-disinformation unit Andriy Kovalenko, Google representatives reached out to Ukrainian government officials to address the issue shortly thereafter.[102]

Similar in many ways was the SpaceX effort to restrict use of the Starlink satellite network close to the active front of the war. Though controversial in the public eye, and significant for military operators and planners, the SpaceX decision to restrict the use of Starlink devices near the front was an intentional one—to limit escalation directly supported by their devices. SpaceX President Gwynne Shotwell explained "our intent was never to have them use it for offensive purposes."[103] The Starlink network, despite these imposed limitations, has undeniably been an extremely useful tool for the Ukrainian military,[104] but its network also supports a much wider geography of users, from individuals to government entities. The inherent dual-use nature of the Starlink network poses a much greater risk should its network be considered a military object. This risk framework is likely a significant part of the drive behind Space X's creation of Starshield, announced in early December 2022. A partner project to Starlink, Starshield operates on a separate network and is specifically and exclusively for government—rather than consumer and commercial—use.[105] With this application in mind, reports still vary as to whether such a contract, like the $1.8 billion deal with the National Reconnaissance Office, would be operated by the contractee, in this case the NRO, or whether, like Starlink, the service would remain operated by SpaceX.[106] It is possible that this case will follow, in practice, the principle that the closer that the operation of a technology sits to strategic and sensitive national priorities, the higher the risk for both state and company of that technology being operated by said company, and the more likely that technology will come to be operated from within a government body.

99. Rachel Lerman, "On Google Maps, Tracking the Invasion of Ukraine," *The Washington Post*, February 25, 2022, https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/.
100. Marc Cieslak and Tom Gerken, "Ukraine Crisis: Google Maps Live Traffic Data Turned Off in Country," *BBC News*, February 28, 2022, https://www.bbc.com/news/technology-60561089.
101. Interview with government affairs executive at US multinational technology corporation, date withheld.
102. Seb Starcevic, "Ukraine Slams Google for Revealing Location of Military Sites," *Politico*, November 4, 2024, https://www.politico.eu/article/ukraine-google-reveal-location-military-site/; James Kilner, "Google Maps 'reveals location' of Ukrainian military positions," *The Telegraph*, November 4, 2024, https://www.telegraph.co.uk/world-news/2024/11/04/ukraine-angry-google-maps-reveal-location-military-position/.
103. Alex Marquardt and Kristin Fisher, "SpaceX Admits Blocking Ukrainian Troops from Using Satellite Technology," *CNN*, February 9, https://www.cnn.com/2023/02/09/politics/spacex-ukrainian-troops-satellite-technology/index.html.
104. "Russia Using Thousands of SpaceX Starlink Terminals in Ukraine, WSJ says," *Reuters*, February 15, 2024, https://www.reuters.com/world/europe/russia-using-thousands-spacex-starlink-terminals-ukraine-wsj-says-2024-02-15/.
105. "Starshield," SpaceX, accessed October 20, 2025, https://www.spacex.com/starshield/; Joey Roulette and Marisa Taylor, "Exclusive: Musk's SpaceX Is Building Spy Satellite Network for US Intelligence Agency, Sources Say," *Reuters*, March 16, 2024, https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/.
106. Tim Fernholz, "The Big Questions About Starshield: SpaceX's Classified EO Project," *Payload*, March 22, 2024, https://payloadspace.com/the-big-questions-about-starshield-spacexs-classified-eo-project/; Brian Everstine, "SpaceX: DoD Has Requested Taking Over Starship Individual Missions," *Aviation Week* Network, January 30, 2024, https://aviationweek.com/space/spacex-dod-has-requested-taking-over-starship-individual-missions; Sandra Erwin, "Pentagon Embracing SpaceX's Starshield for Future Military SATCOM," SpaceNews, June 11, 2024, https://SpaceNews.com/pentagon-embracing-spacexs-starshield-for-future-military-satcom/.

Physicality

Products and services that require the physical presence of personnel, products, or infrastructure within Ukraine are the riskiest to undertake. Providing support in this way carries a level of risk that most companies did not have either the willingness or the infrastructure to take on.[107] While some companies, for certain products, chose to partner with government entities to deliver products or services where physical presence was necessary, as in the preceding example, others chose instead to eschew options with such a requirement. In an interview, one expert said, "there were some products that you wanted to go forward with, but you couldn't. Your informational security can only be as good as your physical security, so projects requiring new physical infrastructure development, or new infrastructure dependencies, was a major stumbling block."[108]

Russia's cyber-offensive impact

To some degree, most of the technology companies in question—especially those with a preexisting presence in Ukraine—were already a target of a significant volume of Russian cyber intrusion attempts as well as other coercive actions. As one industry executive put it when asked about the role of risk assessment in decisions to deepen their work in Ukraine following the invasion, "we knew the risk, we were already targeted on a daily basis."[109] The risk of Russian aggression and retaliation remains, but for many large tech companies, their work already took them into spaces where they were in direct or indirect conflict with Russian or Russian-affiliated groups. However, the risk of Russian cyber intrusions against their networks was already a built-in calculation for their existing cybersecurity plans.

In addition to the experience and expectations of many of these private companies, Russian cyber operations accompanying and following its February 2022 invasion were less disruptive than previously anticipated. The most prominent case of coordinated disruption in the information space remains the ViaSat satellite communications system hack during the invasion. As cyber scholar Jon Bateman writes, this intrusion demonstrated clear "timing (one hour before Russian troops crossed the border), clear military purpose (to degrade Ukrainian communications), and international spillover (disrupting connectivity in several European countries)."[110] However, the incident appeared to be limited in duration and unclear in impact—senior Ukrainian official Victor Zhora acknowledged the loss to communications during the early hours of the invasion, but later stated that the incident was less disruptive than it could have been because of redundancies in Ukrainian communication methods.[111]

As nonresident senior fellow Justin Sherman explored in May 2025 Atlantic Council report, Unpacking Russia's cyber nesting doll,[112] the comparably muted effectiveness of Russian cyber operations during the war is the result of a multitude of factors including:

- Cross-domain coordination difficulties
- Resource constraints
- Interagency competition
- Intentional strategic prioritization
- Ukrainian defensive strength

Sherman goes on to explain that while cyber operations against Ukraine did not have that catastrophic impact expected by some—the promised cyber Pearl Harbor—Russian cyber capabilities should not be underestimated.[113]

In just the first year of the war, Russia and—importantly—non-state actors in Russia's orbit, launched a multitude of cybe-

107. Interview with information security executive at US intelligence and data analysis software technology corporation, May 8, 2024; Interview with government affairs executive at US multinational technology corporation, March 1, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

108. Interview with information security executive at US intelligence and data analysis software technology corporation, May 8, 2024.

109. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

110. Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications, Carnegie Endowment for International Peace*, December 16, 2022, https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

111. Rafael Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset—Ukrainian Official," *Reuters*, March 15, 2022, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/; Kim Zetter, "ViaSat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," *Zero Day* (Substack), September 26, 2022, https://www.zetter-zeroday.com/viasat-hack-did-not-have-huge-impact/; Emma Schroeder with Sean Dack, *A Parallel Terrain: PublicPrivate Defense of the Ukrainian Information Environment, Atlantic Council*, February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

112. Justin Sherman, *Unpacking Russia's Cyber Nesting Doll, Atlantic Council*, May 20, 2025, https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/.

113. Justin Sherman, *Unpacking Russia's Cyber*.

rattacks and intrusions against the public and private sector in Ukraine—including those entities relying on products, platforms, or infrastructure owned and operated by Western tech companies.[114] In May 2025, the US Cybersecurity and Infrastructure Security Agency released a joint cybersecurity advisory highlighting this threat, and explicitly calling out Russian targeting of "those involved in the coordination, transport, and delivery of foreign assistance to Ukraine."[115] The question at hand, then, is not what level of risk is associated with these actions but how prepared the company is to encounter such risks.

Reaction – Risk definition and mitigation

In response to the risk of Russian retaliatory action, either through cyber or kinetic means, states and intranational bodies had a role to play in helping companies to navigate and mitigate these risks. The first method by which this was attempted was in an increased clarity on the types of actions that may be considered military or escalatory in nature. Additionally, in many cases states were necessary partners in securing any element of product delivery or operation required new physical presence in or movement into and across Ukraine.

Definition

Throughout the conflict, industry executives and civil society displayed a great deal of concern about where the line falls between civilian actors and military objectives, and how to ensure that their activities fall squarely on the civilian side of this line. Individuals and companies reiterated a desire for increased clarity on this question from Western governments and international legal bodies.[116] Current humanitarian law requires the country at war to target only military objects, defined as objects "whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" in a manner proportional to the military gain foreseen by the operation.[117]

In a 2023 report, the International Red Cross posited that, "tech companies that operate in situations of armed conflict should understand and monitor whether the services they provide may amount to a direct participation in hostilities by their employees and whether the company might qualify as a military objective."[118] Essentially, the line between civilian and military object is determined by Russia in its assessment of the battlespace, as well as the broader question of whether the Kremlin is concerned about staying within the bounds of international humanitarian law. The subjectivity of this divide allows for some range in interpretation.[119] Indeed some, like Lindsay Freeman at UC Berkeley School of Law, argue that "civilian objects have been intentional, direct targets and not simply collateral damage."[120] Ukraine and its allies cannot simply dictate where such a line exists. However, greater clarity from national and supranational entities would provide some measure of cover to these companies and help solidify their ability to make more accurate risk calculations.[121]

Mitigation

For products and services that require physical presence, either of people or products, many companies view some kind

114. Shane Huntley, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," Threat Analysis Group blog (Google), February 16, 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

115. "Russian GRU Targeting Western Logistics Entities and Technology Companies," Cybersecurity and Infrastructure Security Agency, May 21, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

116. Industry executive, "IT Coalition" Roundtable, Atlantic Council, February 21, 2024; Interview with government affairs executive at US multinational technology corporation, March 1, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024; Interview with information security executive at US intelligence and data analysis software technology corporation; Interview with threat intelligence executive at US multinational digital communications technology corporation, July 26, 2024.

117. International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I),* (June 8, 1977), United Nations High Commissioner for Refugees, https://www.refworld.org/docid/3ae6b36b4.html.

118. *Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations*, ICRC Global Advisory Board on Digital Threats during Armed Conflict, October 19, 2023, https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict, 15.

119. Zhanna L. Malekos Smith, "No 'BrightLine Rule' Shines on Targeting Commercial Satellites," *The Hill*, November 28, 2022, https://thehill.com/opinion/cybersecurity/3747182-no-bright-line-rule-shines-on-targeting-commercial-satellites/; Emma Schroeder and Sean Dack, *A Parallel Terrain: PublicPrivate Defense of the Ukrainian Information Environment, Atlantic Council*, February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

120. Lindsay Freeman, "Evidence of Russian Cyber Operations Could Bolster New ICC Arrest Warrants," *Lawfare*, March 13, 2024, https://www.lawfaremedia.org/article/evidence-of-russian-cyber-operations-could-bolster-new-icc-arrest-warrants.

121. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.

of partnership with government, local or otherwise, as a virtual necessity to bridge the risk imposed.[122]

Cisco's Project PowerUp, led by Senior Security Strategist Joe Marshall of Cisco Talos Intelligence Group,[123] is a clear demonstration of this. The project innovated and delivered a new industrial ethernet switch that could ensure continued effective power grid management even when Russian GPS jamming blocked Ukrenergo substation synchronization, and avoid the resulting forced outages across the Ukrainian power grid.[124] The delivery of these devices into Ukraine was coordinated via a phone call to a US government official who coordinated the first shipment on an upcoming cargo shipment to Poland and then onto a train into Ukraine to be installed by Ukrenergo engineers.[125] While this project was conceived of and executed by Cisco employees, those involved in the project emphasized the importance of Cisco's partnership with the US government on this, as well as other private assistance programs.[126]

Several governments and international organizations have established insurance programs, particularly political risk insurance to help shield companies from the financial risk of investment into Ukraine. In 2023, the Multilateral Investment Guarantee Agency of the World Bank issued guarantees of $9.1 million to support the construction and operation in the M10 Industrial Park in Lviv.[127] Additionally, the US International Development Finance Corporation has established several financial packages guaranteeing millions in political risk insurance for a variety of projects.[128] Within Ukraine, war and political risk insurance is offered by the Export Credit Agency, which insure loans for qualifying Ukrainian businesses against such risks, as well as for direct investment from or into Ukraine.[129] The Ukrainian Ministry of Economy also drafted a law, in cooperation with the National Bank of Ukraine, which would create a unified framework for political or war risk insurance, with a focus on mitigating risks that may deter foreign investments.[130]

The physical element of presence in Ukraine and especially near the battlefield remains a clear demarcation between activities that are the realm of the public sector and those that are the realm of the private sector. In this area, cooperation and coordination between companies and governments could largely follow established practices and procedures. But, for technology whose infrastructure does not touch the territory of Ukraine, the question of where the line is between civilian product and military object, and where bodies like NATO, the European Union, and the United Nations would define that line to be, resembles a gradual gradient rather than a stark line.

122. Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.
123. Joe Marshall, "Project PowerUp - Helping to Keep the Lights on in Ukraine in the Face of Electronic Warfare," Cisco Talos Intelligence blog, December 4, 2023, https://blog.talosintelligence.com/project-powerup-ukraine-grid/.
124. Joe Marshall, "Project PowerUp;" Interview with threat intelligence executive at US multinational digital communications technology corporation, July 26, 2024.
125. Sean Lyngass, "Exclusive: This Pizza Box-sized Equipment Could Be Key to Ukraine Keeping the Lights on This Winter," *CNN*, November 21, 2023, https://www.cnn.com/2023/11/21/politics/ukraine-power-grid-equipment-cisco/index.html; Industry executive, "Tales from Ukraine" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, November 20, 2024; Industry executive, "Supporting Ukraine's Warfighting Efforts with Digital Capabilities" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, September 13, 2024.
126. Industry executive, "Tales from Ukraine" Roundtable, Embassy of Estonia and the Estonian Ministry of Defense, November 20, 2024
127. World Bank Group, "MIGA Backs Industrial Park in Ukraine," news release, September 28, 2023, https://www.miga.org/press-release/miga-backs-industrial-park-ukraine.
128. US International Development Finance Corporation, "DFC Announces $357 Million in New Political Risk Insurance for Ukraine," news release, June 12, 2024, https://www.dfc.gov/media/press-releases/dfc-announces-357-million-new-political-risk-insurance-ukraine-russias.
129. "Your Business in Ukraine 2025," KPMG Ukraine, March 2025, https://kpmg.com/ua/en/home/insights/2025/03/your-business-in-ukraine.html.
130. "Developments in WarRisk Insurance Products for Investments in Ukraine," Dentons, December 5, 2024, https://www.dentons.com/en/insights/articles/2024/december/5/developments-in-war-risk-insurance-products-for-investments-in-ukraine.

Key takeaways and conclusion

Behind much of the discussions and debates among various groups on the role of the private sector in in the war in Ukraine is a deeper anxiety about the evolving character of warfare as we reach the quarter marker of the twenty-first century. The integration and implementation of new technologies and its effect on the practice of war is familiar territory for theoreticians and practitioners alike, from Douhet's theories on the supremacy of air power to the revolution of military affairs (RMA) school of thought, to those today that focus on the effect of evolving drone tactics on the operation and strategy of war. Less comfortable, however, is the analysis of what changes in technology may mean in practice not just for the conduct of war itself, but more fundamentally for the very nature of actors whose abilities and choices shape the conduct of war.

Over the past few years, private companies, especially technology companies based in North America and Western Europe have made decisions as to whether and how to contribute to the Ukrainian war effort in ways that have greatly impacted the ability of the Ukrainian government to direct and effectuate its own defense. In other words, they have moved beyond the status of resource providers in this conflict toward something more resembling actors in and of themselves, at times approaching the importance of states in their contributions.

Clarity of conflict

The war in Ukraine—especially in the first months and years of the war— was notably less divisive in the court of public opinion in the West than many other contemporary conflicts. The historical context of the Russia-Ukraine relationship, along with the sustained aggression launched against Ukraine for more than a decade prior to this invasion and the nature of the invasion itself, combined with myriad factors including those discussed throughout this report, created conditions conducive to widespread sympathy and support across much of Western Europe and North America. The efforts of the Ukrainian government proactively built on these conditions both before and after the invasion. Ukrainian leaders, Zelenskyy in particular, both publicly and in private conversations with government and private sector representatives, clearly communicated the effects of Russian aggression against Ukraine and the actions undertaken by the Ukrainian government and its people.

Clarity of conflict, as a motivating factor for tech companies' decision-making over the course of this conflict, was important in creating favorable conditions for such choices, but is not determinative. Most important as a lesson applicable in potential future conflicts, is that the seeds that grew these conditions into place were planted well before Russian forces rolled across the Ukrainian borders in February 2022.

Business alignment

Many firms had preexisting operations, employees, or customers in Ukraine—generating both a sense of duty and a pragmatic incentive to safeguard assets and personnel. Firms that were already active in Ukraine, or whose services directly contributed to protecting their employees and customers, were the most proactive and consistent contributors. Additionally, companies could derive direct or indirect benefits from their engagement. Several firms leveraged their involvement as an opportunity for product testing, cybersecurity innovation, and real-world validation of technologies under extreme conditions. In doing so, companies not only supported Ukraine's defense but also advanced their own technical capabilities and reputational standing.

Ukraine's long-term digital transformation further enhanced this alignment. Over the past decade, the government has implemented legal and technical reforms aimed at combating corruption and promoting digital industry growth, positioning the country as a prospective regional tech hub and a credible, innovation-friendly partner. This proactive transformation reassured corporate partners that their investments and assistance could be practicable and impactful.

For future conflicts, states will need to account for business alignment factors as an important driving factor in private sector's decision-making. This includes the uncomfortable, yet important finding that this includes companies' ability to profit, or at a minimum, sustain their operations in a conflict in a way that maintains their organizational health, noting that companies' motivations will not always align with that of the states in which they are headquartered. While moral conviction catalyzed early engagement, sustained corporate involvement in Ukraine depended on alignment between ethical action and business strategy.

Difficulty of coordination

Even amid broad goodwill, the initial months of the war revealed the challenge of coordination. Companies often struggled to identify appropriate Ukrainian counterparts, assess needs accurately, or ensure that their offerings were deployed effectively. Early efforts were marked by confusion—with multiple government offices issuing overlapping requests and little centralized control. As Bornyakov later acknowledged, the early days of outreach "were chaos."

Many of the most significant factors that shaped company involvement were already in place and being acted upon before the February 2022 Russian invasion. Preexisting relationships were key, both as a motivating factor and a facilitating factor, effectively minimizing coordination friction. Additionally, the technological and policy developments well underway before the February 2022 invasion created the appealing Ukrainian

tech landscape and improved coordination necessary once the conflict was underway.

While private companies excelled in speed and agility, governments brought scale, reliability, and regulatory legitimacy. The war illustrated how preparedness for potential future conflicts will depend on preestablished coordination frameworks that merge these strengths—enabling rapid mobilization of technological capabilities, matching private capabilities with public needs in real time.

Risk of retaliation

Providing assistance to Ukraine exposed technology companies to new security risks from cyberattacks, sanctions, or kinetic threats against personnel or infrastructure. The degree of perceived risk—and retaliation—varied depending on each company's exposure, particularly for firms whose technologies had direct military applications or some kind of physical presence.

Ambiguity around international law, cyber norms, and export controls can delay or discourage private assistance. Companies must understand whether providing certain technologies or services could be construed as escalatory, illegal, or sanctionable. Private firms are increasingly targeted in state-level cyber operations. The possibility of retaliation, in any of a myriad of forms, was a serious risk for companies aiding Ukraine; managing and sharing that risk is essential to sustaining long-term cooperation.

To mitigate these risks, Ukraine and allied governments played an essential supportive role, clarifying the boundaries between civilian and military assistance, helping companies avoid escalatory missteps and, in some cases, underwrote contracts or insurance to shield firms from loss. Such measures demonstrate the emerging need for risk-sharing frameworks between states and corporations. In cases where physical operations within Ukraine were necessary, governments provided logistical and security coordination to protect personnel and assets. Such collaboration underscores an emerging model of public-private security cooperation, wherein states and corporations jointly navigate the blurred boundaries between national defense and digital resilience.

If private technology companies' decisions and actions are so impactful to the conduct of war, as they have shown themselves to be, then the character of warfare has evolved in such a way as to require states to likewise evolve in the ways that they provide military assistance and plan for potential future conflicts. The foundation for this evolution needs to be a greater understanding of the factors in the case of Ukraine that most greatly impacted company decision-making regarding their participation, or not, in the conflict space, starting with the four factors identified in this report: those that pulled companies toward cooperation, and those that pushed companies away. By assessing the factors that drove companies' decision-making in Ukraine, states can better plan and prepare for future crises and conflicts—and not leave such critical capabilities, once again, to chance.

About the author

Emma Schroeder is an associate director with the Cyber Statecraft Initiative, part of the Atlantic Council Tech Programs. Her focus in this role is on developing statecraft and strategy for cyberspace useful for both policymakers and practitioners. Her work focuses on the role of cyber and cyber-enabled technology in conflict and crime.

Originally from Massachusetts, Schroeder holds an MA in History of War from King's College London's War Studies Department. She also attained her BA in International Relations & History, with a concentration in Security Studies, from the George Washington University's Elliott School of International Affairs.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org