Workshop Report

Volunteer Force

U.S. Tech Companies and Their Contributions in Ukraine

Authors
Christine H. Fox and Emelia S. Probasco

Workshop Participants
John Allen, Kate Charlet, Richard Danzig, Lisa Disbrow, Sean Gourley, Akash Jain, Morgan Kaplan, Margarita Konaev, Samuel J. Locklear III, Igor Mikolic-Torreira, Dewey Murdick, Mark Newton, Fanta Orr, and Eric Traupe

CSET CENTER for SECURITY and EMERGING TECHNOLOGY

May 2023

Introduction

Since before Russia's invasion of Ukraine, strategists, journalists, and even combatants have noted the ability of U.S. technology companies to influence the course of the crisis there. To explore the relationship between these commercial companies and the U.S. government in light of events in Ukraine, we convened a group of leaders, including from industry and government, to evolve our understanding of what is happening and what that might mean for future conflicts. The group included a roughly even mix of U.S. business and former government leaders, as well as several members of the Center for Security and Emerging Technology (CSET), and a representative of the UK Ministry of Defense.

We began our exploration of these issues in our article *Big Tech Goes to War,* published by *Foreign Affairs* on Oct 19, 2022.[*] This workshop explored many of the issues we raised in this article and added more. The conversation was held under the Chatham House Rule but participants agreed to having their names listed. This workshop report captures the key issues that were discussed.

The Commercial Sector Has an Enormous Capability to Contribute State-like Functions to Governments

The innovative capabilities being developed by U.S. tech companies have the potential to change the nature of international conflicts, as is seen in Ukraine today. There, technology companies have made contributions in cybersecurity, digital services, communications, and surveillance. They are bringing with them some of the most advanced, innovative technologies, and they are engaged with Ukraine's government and military both in-person and remotely.

Significantly, tech companies have been able to act swiftly, more so than any government. A single CEO can decide to turn on a communications satellite, defend software from cyberattacks, or provide state-of-the-art AI processing for Ukraine within days, sometimes hours. Large tech company executives can more easily hold direct discussions where official government representatives are more constrained.

While the lack of tight government-led coordination has opened doors for U.S. tech companies to operate swiftly in ways that support Ukraine, this lack of coordination

[*] The October 2022 *Foreign Affairs* article, *Big Tech Goes to War*, can be accessed here: https://www.foreignaffairs.com/ukraine/big-tech-goes-war.

also poses risks. All of our workshop participants agreed that there is huge value in coordinated actions between tech companies and U.S. government leaders and conversely, significant risks. Our participants warned that the United States can benefit from coming together with industry, or it can stay disconnected at its peril.

Speed: A Feature or a Bug?

All participants agreed that tech companies have the freedom to move swiftly, especially when compared to the U.S. government with its exquisite legal processes and procedures. When they do, they can make immediate and, sometimes, enormous contributions. However, the participants also observed that the speed at which companies can operate, which was previously seen as a feature of working with them, is increasingly being treated as a "bug" by government leaders. Relationships that could be developed into helpful collaborations are becoming adversarial. This antagonistic attitude comes from both the U.S. Department of Defense (DOD) and Congress.

"Ukraine doesn't have an acquisition problem, it has a technology problem. The U.S. doesn't have a technology problem, it has an acquisition problem."

Within the broader national security and intelligence community, the tech company participants observed that government representatives too often adopt the view that any private sector employee is a "dirty contractor" only looking to make more money from the government. This bias shuts down the opportunity for collaboration before it can begin. It can be hard to convince government representatives that industry might actually want to make a contribution. Some participants observed that Ukraine has brought government and industry together but, the day-to-day relationship is often adversarial. In the words of one participant, "it doesn't have to be this hard."

The United States Is Not Organized as a Nation to Leverage Its Tech Sector Advantage

There are boundaries and frictions when it comes to government and industry collaborations. They exist for good reasons and participants were clear that they did not esteem the Chinese model of military-civil fusion, as an example. However, DOD's

careful and methodical approach to contracting makes it very difficult to bring innovative tech solutions into conflicts in a timely way.

Many workshop participants acknowledged that they contributed their capabilities to the conflict in Ukraine on their own, that is, without a formal contractual relationship. However, for companies large or small, the U.S. capitalist system is one in which they are meant to generate revenue—and while they may desire to be altruistic or patriotic, they will eventually be limited by their obligations to their employees, customers, and/or shareholders. As one participant put it, while companies are prepared to compete to win, they cannot compete with "free," at least not for long, and so they need sources of revenue.

While the DOD has good reason to be risk averse when it buys goods and services for the nation's defense, its approach is increasingly built for a different era. Participants were particularly concerned about the DOD's inability to contract software and digital services, which require different interactions between the government sponsor and contractor than do traditional hardware contracts. They were similarly concerned about the government's ability to contract software at speed from contractors who may be new to working with the DOD. Without the benefit of DOD contracting experience or existing contracts, tech companies are hard pressed to help in a crisis. Even with existing contract vehicles in place and funds available, the process can be long and expensive, which effectively eliminates small startups from contributing.

The inability of the U.S. government to contract rapidly for software was made clear in Ukraine—not just because of how nimbly the Ukrainians adopted the software but also because of the clear impact that digital services have on military operations. The full scope of the impact that commercial digital services have on the war in Ukraine is still being studied. However, it seems clear that these services and capabilities are playing a key role in helping Ukraine counter Russia's advances.

The DOD Needs to Build Strong Relationships with Tech Companies, Both Formal and Informal

Without functioning formal relationships, the tech companies relied on informal relationships to take action in Ukraine. There are numerous informal connections in the United States between government and industry that helped to facilitate corporate actions. They range from engagements built by government relations teams to the social relationships of leaders or even working-level collaborations between key employees.

All of these relationships proved crucial in the earliest days of the Ukraine conflict, when both industry and government scrambled to respond to threats and attacks against Ukraine, global infrastructure, and U.S. companies themselves. The relationships helped facilitate cybersecurity efforts and also gave both sides information on how to improve or adjust existing platforms in the context of war in Ukraine. One particularly notable point was that informal relationships with government diplomats, as well as domestic law enforcement, were needed to help companies protect their American employees who were targeted by Russia, regardless of where they were based internationally.

In the absence of more responsive formal contracting relationships, informal connections can fill an important gap that exists between U.S. government and tech companies. All workshop participants expressed the desire for more frequent dialogue and venues for open conversation.

Ukraine is a Model, But Next Time Will Be Different

The U.S. government still has much to learn about the experience of Ukraine and the ways in which technology companies play a role in the conflict. However, depending on tech companies to come forward on their own has significant risks. Participants discussed the uniqueness of the conflict in Ukraine: it is a clear violation of international law and norms by a country with a relatively weak economy and a long history of aggression in the public mind. Moreover, it is taking place in a country near numerous U.S. and allied military bases (not to mention corporate footholds) that have relatively well-established infrastructure and pre-positioned resources. Representatives at the workshop said this context helped company leaders explain and get buy-in from their employees and stakeholders to take action.

"For Taiwan, the cost is high and the imperative is unclear."

But they also said that Ukraine was a more straightforward decision. A conflict over Taiwan would be very different.

Many of the large U.S. tech companies have significant relationships with China. They have R&D labs there, they depend on China for manufacturing key components of their products, and China represents a significant market for them. Ultimately, each

company is beholden to the forces of capitalism for their success and survival. While some companies have made deliberate business decisions that make choosing sides in a conflict a given, many other powerful companies have more complex international relationships and must navigate a web of international markets, rules, and stakeholders. And on top of this, especially with respect to a potential conflict in Taiwan, U.S. tech companies have many employees living in China who could be at risk should those companies become actively involved in defending Taiwan.

When asked what the United States and its allies might do to build a basis for collaboration today, before a potential crisis over Taiwan, the workshop participants from the tech sector had several ideas:

- **Messaging.** Company leaders identified the need for a compelling reason to act. In Ukraine, it was clear that Russia's actions against the country were reprehensible. It was relatively easy for the companies to convince their workforces that taking action was the appropriate response. For Taiwan, the United States has not been as clear in its message. U.S. policy has often been purposefully vague, making it much more difficult to articulate why it is an imperative for a company to act.

- **International consensus.** In the context of Ukraine, company leaders could rely on unified messaging from international leaders about the wrongness of Russia's actions and the need to fight in response. The near unity of opposition internationally proved valuable in a company's ability to convince its employees, shareholders, and customers that its actions were justified and acceptable. International consensus, as well as the statements and actions of international governmental organizations, are especially important for large U.S. multinational companies that must manage global relationships. All tech company participants agreed that a similar international consensus would be important before they could take action in a conflict over Taiwan.

- **Legal actions.** Sanctions and legal frameworks were important actions that, in many cases, simplified decisions for tech companies. In the case of Taiwan, these legal frameworks could be especially helpful and important.

- **Domestic political consensus.** All participants commented on the importance of domestic political consensus. It will be important that the legislative and executive branches pull in the same direction if they are to convince their employees and shareholders of the need to act.

- **Contracts.** For some companies, formal contractual relationships will be even more important in a conflict like the potential invasion of Taiwan by China. Contracts lend appropriate protection to companies and especially company employees during a conflict. The inability of the government to install a contract rapidly puts employees at risk. Contracts also remove the financial risks that a company would face, making participation much more attractive.

- **Pre-positioning.** The pre-positioning of personnel and infrastructure in and around Ukraine helped companies surge resources quickly. It would have been very difficult to establish a presence from scratch in the midst of the conflict. Having observed the importance of pre-positioned personnel and infrastructure, one participant's company has already opened an office in Taiwan.

- **Principles.** Several participants made note of the role pre-established company principles played in guiding their decisions after hostilities began, calling it a "North Star" for action. For example, will they manufacture their products in a country that is a U.S. adversary? Will they export their products to that country? Under what conditions? By answering these types of questions in advance of conflict, companies can evolve their principles so that they are robust for future conflict. For government, fostering conversations with companies today about those principles could help build these important relationships and help government understand the challenges the private sector would face in the potential conflicts of tomorrow.

Conclusion

The workshop participants made clear that this topic has not been examined in depth and that much more deliberation is needed. Some participants observed that there are considerable precedents for government engagement with private corporations. They recommended conducting historical case studies, as well as more current ones, ranging from Cyber Information Sharing and Analysis Centers (ISACs) to the use of contracted airline carriers to support the international evacuation from Afghanistan. These case studies could provide insights into events where public-private partnerships were needed and used effectively. All participants agreed that the lessons from Ukraine need to be captured and shared widely across the public and private sectors.

Most significantly, all participants recommended that a second workshop be held, this time including current government leaders. Ironically, all participants observed that it would be legally challenging for current government officials to meet with commercial contractors for such a discussion. Some participants observed that other countries have fewer restrictions when engaging with contractors. This suggestion points to the significance of international partnerships when it comes to helping the U.S. government and U.S. technology companies have a positive impact in the conflict in Ukraine. Other nations have different rules and processes, sometimes allowing them to move faster. By working together, all players gain an advantage.

However it happens, more extensive and continued conversation is needed. Collaboration and more nimble contracting between the U.S. government and commercial tech companies is imperative. These companies have enormous capabilities. Their actions can be conducted in concert with—or as a detriment to—global security. Conversation, collaboration, and more nimble contracting are all needed urgently.

Authors

Christine H. Fox is a senior fellow at the Johns Hopkins Applied Physics Laboratory. She has previously served as the acting U.S. deputy secretary of defense from 2013 to 2014, as well as the director of cost assessment and program evaluation in the Office of the U.S. Secretary of Defense from 2009 to 2013.

Emelia S. Probasco is a senior fellow at CSET where she works on the military applications of artificial intelligence. She was previously the chief communications officer and communications department head at the Johns Hopkins Applied Physics Laboratory, and a surface warfare officer in the U.S. Navy.

Participants

John Allen

Kate Charlet

Richard Danzig

Lisa Disbrow

Sean Gourley

Akash Jain

Morgan Kaplan

Margarita Konaev

Samuel J. Locklear III

Igor Mikolic-Torreira

Dewey Murdick

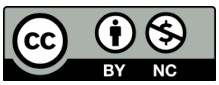
Mark Newton

Fanta Orr

Eric Traupe

Acknowledgments

For feedback and assistance, we would like to thank Sue Gordon. We would also like to thank Danny Hague and Kathleen Curlee for their logistical support and research assistance.



Document Identifier: doi: 10.51593/20230015