GLOBSEC US Foundation

Ukraine's cyber defence: Insights on private sector contributions since the Russian invasion

Anushka Kaushik, Senior Research Fellow & Cyber Lead, GLOBSEC

The following policy brief outlines some key takeaways from the active private sector participation in Ukraine's cyber defences since Russia's invasion in February 2022.

It contains insights from industry experts, government representatives, and researchers on cybersecurity who participated in a closed-door roundtable discussion conducted as part of the GLOBSEC Future of Cyberspace Cooperation Initiative: Transatlantic Chapter.

Introduction

While the cyber domain of conflict has not received as much attention in the war waged against Ukraine, the country has been determinedly building its cyber resilience allowing it to defend in cyberspace as formidably as it has. In part, Ukraine has been able to build resilience by partnering with the private sector as a key ally.

The involvement of technology companies in bolstering Ukraine's cyber defences has been a noteworthy development, highlighting once again how crucial the private sector is in securing cyberspace. A prominent example is the migration of critical Ukrainian data facilitated by key players in the private sector – a few days before the invasion, on Feb 17, 2022, Ukraine authorized **migrating national data** to the public cloud from servers operating entirely within the country. This move was significant as it enabled protection of critical data and is also indicative of Ukraine's prioritizing of cyber resilience – while defenses might be overcome, having a backup for critical data that is separate can **offset the consequences** of an attack. This serves as a valuable lesson on the significant role that the private sector can play in cyber conflict.

Major technology companies have provided technical support to users via **free security services** and collaborated with the Ukrainian government on enhanced threat intelligence sharing and investigations. For example, a destructive malware (**dubbed Industroyer 2**) targeting a high-voltage electrical substation was identified by Bratislava-headquartered company ESET which worked with the Computer Emergency Response Team-Ukraine (CERT-UA) to take remedial action. ESET indicated that this is a new version of Industroyer used in the notorious 2016 Ukrainian electric grid attack that left thousands without electricity. The potential damage that could have been caused by this malware underscores the significance of collaborative efforts between industry and organizations responsible for maintaining critical infrastructure, to ensure the highest level of protection against malicious attacks. Major private sector players continue to work on cyber threat and intelligence exchange and mitigating the impact of cyber-attacks with Ukrainian authorities.

With respect to private sector involvement in cyberspace conflict, policymakers will face numerous challenges in delineating their scope of activities. One critical issue is the lack of clarity regarding the extent of the private sector's involvement in the geopolitical domain, despite its crucial role in defending against hostile actors. This is compounded by growing threats to companies from hostile nation-states and the need that will arise to formulate a strategic response.

Furthermore, to navigate differing incentives of the public and private sectors and address the inevitable sovereignty issues that arise, necessitates a much deeper understanding of the dynamics between the private sector, the public sector, and state actors in the realm of cyber conflict.

Key Takeaways

1. Ukraine's cyber defence campaign is a long-standing and protracted effort to build cyber resilience in its systems. Its own emphasis on institutionalising cybersecurity strategies, partnering with Transatlantic governments and IGOs, scaling its own cyber capabilities and its history of being targeted by Russian cyber-attacks are all factors that have facilitated such a robust response. **Private sector contributions have built upon and complemented this extensive cyber resilience campaign.**

2. Ukraine has partnered with the domestic private sector at two levels – the first is through conscription, where the government has recruited highly qualified technical expertise and at the second level are volunteers from the domestic private sector, volunteering their time and expertise on fields like incident response, building cyber resilient systems among others. **A critical function of these volunteers has been building trust between the Ukrainian government and the private sector[1].**

3. While there is no specific global statistic available on the ownership of critical infrastructure as this varies by country, according to conversations with Ukrainian authorities, more than 50% of the Critical Infrastructure is privately-owned. **Ukraine has leveraged the private sector to protect and build cyber defences of privately-owned critical infrastructure companies[2].**

4. Although questions remain about an institutionalised cyber defence model, **private sector involvement in Ukraine's cyber defence, the cooperation between CERTs, technology companies, and security agencies suggests that ad-hoc collective cyber defence efforts are already underway.** Moreover, as various companies possess distinct information and telemetry on cyber-attacks, sharing this data could notably enhance the collective comprehension of the cyber threat landscape.

5. **Governments are no longer the only prominent stakeholder in intelligence services in the information sphere given the private sector's unparalleled data and telemetry for understanding cyber-attacks and the threat landscape.** Companies involved in preventing and mitigating the impact of cyber-attacks possess invaluable, actionable, and operationally useful intelligence about cyber threats. The government and private sector must devise more efficient ways to cooperate in this sphere. One potential challenge to collaboration is the need to balance the sharing of sensitive information - pertaining to the systems in use and the criticality of data hosted - with the need to protect national security and proprietary information. Additionally, different countries may have different legal and regulatory frameworks governing information sharing, which can make collaboration more difficult.

6. In the absence of clear information disseminated by governments, **the private sector is emerging as a reliable source of information on understanding threats in cyberspace and are contributing to shaping the public perception of conflict in this domain.** For example, leading technology companies have released detailed reports on Russian cyber tactics against Ukraine, leveraging their vast cyber threat data to present easily understandable insights.

7. The anticipation of private sector cyber firms collaborating with the government to protect against cyber-attacks on data and critical infrastructure raises important considerations regarding the implications for international law of conflict. **The application of norms governing their actions in cyberwar, the need for limitations on a cyber attacker's ability to target private cyber defense firms, like the restrictions imposed on attacks on civilians in general, and whether firms could be regarded as combatants are issues that require further study.**

8. There is a gap in conversations around the public-private collaboration in Ukraine's cyber defences - that is, **the impact on small companies**

1 Based on conversations with Ukraine's State Service of Special Communications and Information Protection of Ukraine (SSSCIP)
2 Based on conversations with Ukraine's SSSCIP

that do not possess enough information on cyber threats and are not part of existing partnerships that would enable access to such intelligence. Small companies often have limited resources and may not have the budget to invest in robust cybersecurity measures, increasing their vulnerability to cyber-attacks. They are also easier targets of cybercrime groups, making their partners equally vulnerable. In that regard, the onus to provide basic cybersecurity must be on governments and larger cybersecurity providers to reduce overall risk.

9. **Establishing a mechanism to monitor technological aid extended to Ukraine** is a crucial area where public-private collaboration is necessary. During GLOBSEC's discussions with industry, instances where Transatlantic governments have approached significant technology players seeking verification of entities purporting to provide technical support were discussed. It is imperative to obtain a more comprehensive understanding of the type of support being offered and the degree of involvement.

Conclusion

Ukraine's campaign to build its cyber resilience has been extensive, and the involvement of the private sector has been instrumental in this regard. By partnering with technology companies, Ukraine has been able to access critical cybersecurity tools and intelligence, which has complemented its own cyber defence efforts. Domestically, Ukraine's engagement with the private sector has been particularly significant in protecting privately-owned critical infrastructure companies and building trust with the government. However, challenges remain in delineating the scope of private sector involvement in cyber conflict and navigating the differing incentives of the public and private sector. These challenges are also roadblocks to any feasible institutionalised cyber defence model, even as the level of cooperation between CERTs, technology companies, and security agencies suggests that ad-hoc collective cyber defence efforts are already underway.

On a Transatlantic basis, Allies need to work together particularly with global private sector enterprises to come with up joint strategies in securing the Internet. Most recently, the **US National Cybersecurity Strategy 2023** has signalled the importance of public-private partnerships to ensure the security and resilience of critical infrastructure, seeking to increase the responsibility of critical infrastructure owners/operators to adopt measures that better secure their cyber capabilities. Additionally, the private sector's access to telemetry for understanding cyber-attacks and the threat landscape at an unparalleled level and its capabilities to innovate must be leveraged by governments.

This brief is published as part of the GLOBSEC Future of Cyberspace Cooperation Initiative - Transatlantic Chapter which aims to assess key regional and global partnerships in the field of cybersecurity and provide concrete roadmaps for the future. With increasing cyber insecurity, a changing threat matrix, and unprecedented geopolitical circumstances, the significance of building partnerships to further common cybersecurity goals cannot be overstated. The Initiative seeks to carry out these assessments in three parts - the ***Transatlantic Chapter, Pan-European Chapter, and the Central Eastern and European Chapter.***

GLOBSEC would like to thank the core committee members of the Future of Cyberspace Cooperation Initiative – Michael Chertoff (Chairman, The Chertoff Group), Melissa Hathaway (President, Hathaway Global Strategies LLC), Andrew Lee (Vice President of Government Affairs & Global CTI Strategist, ESET), and Lukas Hlavicka (CTO, ISTROSEC) for their inputs and support.

In partnership with GLOBSEC US Foundation.