YOUNG LEADERS PROGRAM

THE ROLE OF THE PRIVATE SECTOR IN CYBER COMPETITION

BY *BRONTE MUNRO*

Bronte Munro *(brontemunro@aspi.org.au) is an Analyst at the Australian Strategic Policy Institute (ASPI) Washington DC.*

The Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) workshop on *'The future of cyber competition'* was held to further an understanding of what lessons the US, and its allies, could take from how cyber has been used during Russia's war on Ukraine. Discussion between senior US government officials, private sector experts and academia over the two days was key in highlighting that it is important to define what successful public-private partnerships look like, and how effective relationships can be built to best prepare for future conflict.

The importance of public-private partnership is at the forefront of policy debate as global technology competition continues to intensify. The passing of legislation in the United States, such as the CHIPS and Science Act 2022, aimed at securing semiconductor supply chains, and inquiries by Senators into Elon Musk reportedly thwarting a drone attack on Russian targets by denying the use of SpaceX's Starlink satellites, is indicative of the undeniable presence of the private sector in strategic competition and global conflict. Going forward, US and allied governments need to make considerations around the normative parameters for collaboration and private sector engagement in cyber conflict, particularly given critical digital infrastructure and large troves of personal data is largely operated and managed by private sector entities.

A point raised throughout the CGSR workshop, was that strengthening and encouraging the private sector's ability to act in geostrategic competition is not necessarily a status quo that should be reinforced. 'Big tech' companies are in some instances, operating with the scale and influence of countries, as is the case with SpaceX, which has been central in providing critical communication infrastructure during the Ukraine war. These companies are not bound to national interests and typically view themselves as international organisations headquartered around the world with their primary activities driven by commercial interests. This perspective was raised in conjunction with the point that while Ukraine has demonstrated an adept ability to use soft power to harness private sector support, this is not necessarily replicable in future conflicts. The US and allies need to consider if it is within their interests to normalise the independent involvement of private sector entities with the capacity to function on the scale of a combatant country during conflict particularly in a scenario where a large private entity might aid a foreign adversary.

Regardless, while the nuances of the normative parameters for private sector involvement in geostrategic competition are still developing, the private sector will continue to hold an integral role in cyber and technology competition. Another key point emphasised during the workshop, was the importance of developing a roadmap for engagement and timely communication between government and the private sector. The war in Ukraine has highlighted the need to have these strategies in place prior to a conflict, as opposed to being built mid-flight. Related to this, is the importance of building the skills within both public and private sectors to effectively communicate in technical areas to non-technical audiences, and vice versa when it comes to explaining strategic policy priorities and how the technical capabilities of the private sector might support them. Cyber is a multidisciplinary field, and having individuals that can act as a conduit between technical and high level geostrategic or commercial audiences is vital, and is a function that should exist ahead of a cyber conflict scenario. The private sector is not a uniform entity, and trust and relationships at an individual level need to be built between public and private entities if constructive collaboration is to occur. Building these relationships will also help identify scenarios where

collaboration is needed, and the degree of risk appetite and priorities for both the government and private sector entities. This feeds into a need for public-private partners to candidly understand each other's unique incentives, which the CSGR workshop was clear in highlighting as important for ensuring partnerships of value can be built.

This is where there is an opportunity for greater collaboration between allies and learning from different approaches for public-private engagement in cyber. Notably, Australia is at the forefront of public-private collaboration in scenario planning for major cyber incidents. In 2023, the Australian government held war gaming exercises with major banks and financial service companies to test response strategies to cyberattacks that target critical infrastructure assets. How allies can execute similar programs to work in tandem with global companies to drill scenarios and understand the capabilities, intentions, and limits of private sector entities will help lay the groundwork when real-time responses are needed.

For the private sector, engaging in these activities does not necessarily commit them to supporting a government position during a conflict, but enables them to define the parameters of their willingness to collaborate prior to the fact, build useful relationships and trust, and think through any legal and public relations considerations they might face.

The CSGR workshop was key in highlighting that in the man-made domain of cyber, collaboration is vital, both with allies and the private sector. As geostrategic competition in the Indo-Pacific continues to intensify, China will also be looking to the lessons of Russia's invasion of Ukraine to determine where improvements to their utilisation of cyber as a tool for information warfare and disruption can be improved. China's relationship with the private sector differs greatly to the US and its allies, where China has a higher degree of integration. While discussion at the CSGR workshop raised the point that this reduces China's private sector's ability to act quicky, be agile and innovative in their activities and responses, it did not diminish the fact that the US and partners should continue to collaborate to improve their readiness in the ever-changing cyber domain.

Disclaimer: All opinions in this article are solely those of the author and do not represent any organization.