YOUNG LEADERS PROGRAM

CYBERSECURITY WORKSHOP

BY *AYAE YOSHIMOTO*

Ayae Yoshimoto *(ayeysmt@gmail.com) is a researcher at the Consulate General of Japan in San Francisco, California.*

In the realm of cybersecurity, 'The Future of Cyber Competition' workshop, hosted at the Lawrence Livermore National Laboratory's Center for Global Security Research on September 12th and 13th, emerged as a pivotal gathering. This workshop served as a focal point for professionals and scholars immersed in the dynamic and ever-evolving landscape of cybersecurity policy. Notable attendees included representatives from the U.S. government, international organizations, and a diverse array of experts from the private sector, all of whom contribute significantly to various facets of cybersecurity. The workshop offered a rare opportunity for these stakeholders to engage in an extensive dialogue about the future of cybersecurity.

Each panel introduced intriguing subjects, including insights from Ukraine's experiences, strategies concerning cybersecurity in partnership with U.S. allies, and the intricate interplay between information and technology competition. Amid the discussion, a compelling trend emerged – discussions consistently converged towards the topic of collaboration with the private sector.

Indeed, the emphasis of the discussions on collaboration with the private sector is entirely understandable. The cybersecurity domain, still regarded as a relatively recent addition to the broader spectrum of national security, has yet to reach its full maturity. This nascent state of affairs became evident as the United States unveiled its inaugural Cyber Strategy on the eve of the workshop. Unlike well-established norms and frameworks found in traditional security domains, the world of cybersecurity lacks a universally accepted definition, and the formation of international norms and frameworks remains a work in progress. Moreover, the application and efficacy of cybersecurity measures remain subjects of limited research, owing to the paucity of comprehensive case studies. As such, caution must be exercised when extrapolating insights gleaned from specific cases, such as Ukraine, to construct universal principles in the multifaceted realm of cybersecurity. The reality is that there is still much we do not understand about the intricate nature of cybersecurity.

Paradoxically, the Ukrainian case serves as a compelling illustration of the influential role that non-state actors, primarily from the private sector, play in the domain of cybersecurity. In contemporary international conflicts, non-state actors wield an unprecedented degree of influence, a departure from the traditional dynamics observed in conflicts and wars. Panel discussions during the workshop underscored the stark contrasts between non-state actors within the private sector and the actions of nation-states. The differences between the private sector and nation-state actors are too numerous to enumerate comprehensively, yet a fundamental distinction arises from the motives behind their actions: nation-states act with the overarching goal of safeguarding and advancing their national interests, while the private sector operates under the primary objective of profit maximization. Consequently, the reliability of the private sector can exhibit considerable variability, which poses challenges, especially in times of crisis, such as a hypothetical Taiwan Strait contingency. Nonetheless, it is crucial to recognize that effective cybersecurity policy must strike a delicate balance. Given that the private sector possesses advantages in terms of scale and speed, collaboration with the private sector cannot be avoided. Therefore, it is essential to thoroughly examine how to integrate collaboration with the private sector into government cybersecurity policies.

Furthermore, the workshop's discussions remarkably did not extend to the crucial aspect of cooperation and collaboration among allied and partner nations. Nonetheless, due to the inherent ambiguity of the field

and its capacity to transcend various domains and national boundaries, it can be argued that international cooperation and collaboration among countries becomes a necessity.To foster and enhance international cooperation and collaboration in the domain of cybersecurity, several essential steps must be taken. First and foremost, there is an imperative need to establish a comprehensive and universally agreed-upon understanding and delineation of what precisely cybersecurity entails. This foundation should be buttressed by the development of international norms and frameworks, providing a robust structure for the multifaceted cybersecurity arena. Equally important is the establishment of mechanisms for intergovernmental cooperation and collaboration, which would form the bedrock of effective cybersecurity strategies. Moreover, a wealth of practical case studies, encompassing diverse scenarios, is essential to enrich our collective knowledge base. These studies will serve as invaluable reference points for policymakers, practitioners, and academics alike.

The discussions surrounding national security often gravitate towards the conventional threats and risks associated with territorial defense and military strategies. While these conventional concerns remain of utmost importance, it is imperative that the United States, its allies, and its partners acknowledge the increasing significance of non-traditional security domains, chief among them being the realm of cybersecurity. In this rapidly evolving landscape, a robust framework for cooperation and a shared understanding of the complexities involved are paramount. A strategic shift is necessary to address the full spectrum of security challenges, encompassing traditional and non-traditional threats alike.

Cybersecurity is inherently interconnected, transcending borders, industries, and sectors. It is a dynamic field that continually evolves, presenting a challenge that cannot be adequately addressed by any one nation or entity in isolation. Therefore, it is imperative for like-minded nations to collaborate not just in the realms of defense and intelligence sharing but also in the realm of cybersecurity.

In conclusion, the 'Future of Cyber Competition' workshop offered a glimpse into the multifaceted and dynamic world of cybersecurity. It underscored the critical importance of collaboration, particularly with non-state actors in the private sector. Furthermore, it highlighted the nascent nature of the field, which calls for further research, the development of international norms, and the cultivation of effective mechanisms for cooperation among nations. To navigate the uncharted waters of cybersecurity successfully, a shared commitment to understanding, cooperation, and collective action is indispensable.

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