TLS Symposium Summary: “Russia-Ukraine: The Cyber Dimensions”

Co-Authored by: Lauren Mantel & Jackson Colling

Moderated by The Washington Post’s Ellen Nakashima, the symposium's opening panel, "Russia-Ukraine: The Cyber Dimensions," featured Ivan Kalabashkin from the Cyber Security Department of the Ukraine SBU, Pete Renals from Palo Alto Networks, and Fanta Orr from Microsoft. The panel primarily focused on how Russia and Ukraine are utilizing their cyber capabilities in the ongoing war and how they have both adapted their cyber capabilities and strategies over time. The panel also touched on the private sector’s role in the war thus far.

The panel began with a conversation about Russia’s pre-invasion cyber operations against Ukraine. Before Russian troops crossed into Ukraine, Russia launched FoxBlade, a cyber-attack with a piece of wiper malware, and a range of other cyber operations against Ukraine. These operations did not achieve their intended effects of sowing fear and taking down Ukrainian networks, showing the resilience of Ukrainian cyber defenses and previewing the role the private sector would play in helping Ukraine detect and defend against cyber threats.

The panelists then discussed how Russia’s war on Ukraine can be categorized as the first cyber war in history and that this war is the first time the world has witnessed a hybrid war at this scale. Highlighting this point, the panel spoke about the frequency of Russian cyber operations, with over 3,000 operations neutralized this year. Mr. Kalabashkin discussed how Ukraine has been building its cyber capabilities since 2014 by learning from Russia’s constant bombardment of its systems, resulting in a resilient Ukrainian network. Further, at the onset of Russia’s invasion Ukraine quickly replaced legislation preventing data migration with one that permitted it. This strengthened Ukraine’s networks in that it mitigated the threat of Russian kinetic attacks on servers while granting greater access to private-sector protection efforts.

Discussing Russia’s evolving strategy, the panel addressed the ineffectiveness of Russian cyber operations and how Russia’s target selection has changed. Mr. Kalabashkin highlighted how Russia has pivoted from initially targeting critical infrastructure to now utilizing cyber for intelligence gathering and reconnaissance. The panel discussed Russia’s return to targeting critical infrastructure as the fall/winter approaches and that Russia will likely combine cyber operations with kinetic attacks to amplify the effects on critical infrastructure. Finally, the panel spoke about how attacks have evolved from opportunistic to targeted attacks, Russia’s progressing national cyber offensive program, and the new challenges of younger individuals with looser ties to Russia perpetrating attacks against Ukraine.

Focusing on the private sector, the panel discussed the importance of building cyber resilience through public-private partnerships and how it has been integral to building Ukrainian cyber resilience. Mr. Renals observed how conflict can swiftly drive significant change and reflected on Ukraine’s change in data migration laws and the private sector refining how and what it provides to Ukraine to amplify effectiveness. The Panel emphasized that companies, like Microsoft and Palo Alto Networks, augmented existing Ukrainian infrastructure in place since 2014. Ms. Orr discussed how Microsoft shifted its threat intelligence in the fall of 2021 to focus on Russia’s potential invasion and established secure lines of communication with Ukraine after discovering malware in January 2022. Now, the threat intelligence unit is utilized to quickly spot Russian activity and rapidly provide information to Ukrainian elements who can action the intelligence and leverage domestic resources.