Under Secretary Silvers Speech at the 2023 Munich Cyber Security Conference: Transformational Cyber Defense at the International Level

February 17, 2023

Remarks as Delivered

Good morning and thank you very much.

We need transformational change in how we build cyber defense at the international level. It is no longer enough to have meetings and declare partnership.

Together, we must move hard toward operational collaboration between governments and the private sector, as well as among national governments. The Biden-Harris Administration is leading this transformational change in how we defend our networks.

We see this in how governments and industry have come together in support of Ukraine, which has faced an onslaught of Russian cyberattacks on both civilian and military infrastructure accompanying Vladimir Putin's brutal invasion.

As Russian forces began to mass on Ukraine's borders, making clear an invasion could be imminent, governments and companies surged in to help Ukraine bolster its digital defenses. Technology and cybersecurity companies began working with the Ukrainian government and critical infrastructure operators to build redundancy and resilience, and positioned Ukrainian network defenders to better detect and repel threats to critical infrastructure.

Partner governments also stepped in proactively, including cyber teams from across the U.S. government. At the Department of Homeland Security, we have worked closely with the Ukrainian Ministry of Digital Transformation in support of its mission to protect Ukrainian infrastructure. Our Cybersecurity and Infrastructure Security Agency, or CISA, has increased cyber threat information sharing, stepped up expert-to-expert exchanges, and provided hands-on training on securing industrial control systems.

This all-hands effort to repulse Russian cyber threats to Ukraine shows the power of investing in partnerships and preparedness, even in the face of the most sophisticated adversaries. Ukraine has cut off at the pass a number of serious, attempted intrusions and disruptive attacks in a way that few would have predicted before the invasion. Some cyberattacks have succeeded to be sure, but Ukraine's cyber defenses have been much more robust than expected.

The war in Ukraine teaches us that defense matters. Resilience matters. Our relationships matter. We have seen that doing the hard work on the front end pays off – company to company, government to company, and government to government. We are acting on these lessons globally.

DHS is seizing every opportunity to deepen our partnerships between national governments.

We have broken new ground with the expansion of the Abraham Accords to include cybersecurity. Just a couple of weeks ago in Tel Aviv, I had the honor of joining the leaders of

the cybersecurity agencies of Israel, the United Arab Emirates, Bahrain, and Morocco to advance cyber defenses and resilience across the Middle East.

DHS will be working with these countries to bolster critical infrastructure protection and network defense. All our countries face common threats, not least from Iran and cyber criminals that select targets around the region and the world. We think this is an important new model for tackling cyber challenges at the regional level.

Our defensive cybersecurity collaboration in the Middle East has already paid dividends. Through these new channels, we have received actionable technical information on shared cyber threats and vulnerabilities, including on specific cyber activity targeting critical infrastructure.

We have held joint tabletop exercises simulating cross-border cyberattacks. More joint defensive activities will follow, to the benefit of the populations across our countries – another dividend generated by the geopolitical shifts that we are capitalizing on to protect our people and critical segments of our economies.

Our international cybersecurity collaboration of course stretches beyond the Middle East, from our extensive intelligence sharing amongst the Five Eyes and European partners to our newly forged partnership with Japan to efforts we plan to undertake in the Western Hemisphere.

To address the most intractable cybersecurity challenges, the Biden-Harris Administration is delivering global solutions.

The Administration's Counter Ransomware Initiative brings together 36 countries and the EU to counter the global ransomware scourge. Together, we are going after ransomware actors, disrupting their safe havens, seizing illicit profits, sanctioning cryptocurrency exchanges that turn a blind eye to ransomware-related transactions, and preventing the misuse of commercial infrastructure to launch attacks.

This is a combined effort of network defenders, law enforcement, financial system regulators, and more – all across the globe.

The United States is an active participant in the Initiative's new, Australian-led International Counter Ransomware Task Force, which will be a focal point for member countries to disrupt ransomware actors and to work with the private sector to build resilience and defend their networks.

Transforming cyber defense at the international level is not only about how we collaborate to address the threats of today. We must also look back to learn how we can better defend ourselves against the threats of tomorrow.

Last year, we launched the Cyber Safety Review Board, the CSRB, to conduct after-action reviews of the most significant cybersecurity incidents and publish recommendations so that the community can learn from past experiences.

The Board has equal membership from cyber leads from our federal government on one hand, and private sector security luminaries on the other. I am pleased to chair this unprecedented

public-private partnership, which has become an enduring fixture in our cybersecurity ecosystem.

The CSRB's reviews are already raising the bar for cybersecurity in the United States and around the globe.

Last year, the Board published its inaugural review of the Log4j vulnerability, one of the most significant open-source vulnerabilities in history, which affected systems all around the world.

The review benefited from engagement with more than 80 organizations, including government counterparts from the UK and Israel.

The Board indeed received a response and conducted an interview with representatives of the government of the People's Republic of China, although their input still left a number of questions unanswered about their concerning response to the vulnerability's disclosure.

Thanks in no small part to the international character of its fact-finding, the Board was able to establish a definitive timeline of the Log4j discovery and provide actionable recommendations for both governments and industry to bolster open-source software security, respond to major incidents, and sustain vigilance against exploitation of this endemic vulnerability.

The CSRB has now been charged with reviewing a spate of extortion-based attacks associated with hacking groups like Lapsus$, which have impacted some of the biggest and most well-defended companies in the United States and around the world. Additionally, according to threat intelligence experts, many of the perpetrators are based in countries that cooperate with Western law enforcement requests. So we have lessons to learn about how to protect against, and disrupt, these kinds of criminal outfits on a global basis.

The Board will continue to tackle the most significant global cyber incidents and trends, bringing together the best expertise from the public and private sectors for the benefit of the entire global cybersecurity community.

The threat environment we face demands operational collaboration across borders, industries, and governments to build a true architecture of security around our vibrant digital societies. This is how we will achieve transformational change in the way we build our global cyber defenses.

Thank you.

###