Secretary Mayorkas Remarks:
The Convergence of National Security and Homeland Security

Release Date: December 5, 2022

Transcript:

In June of 2017, Russia launched the NotPetya cyber-attack against Ukraine, causing indiscriminate impacts to a wide range of organizations, from banks and government ministries to electricity companies. The majority of attacks affected organizations in Ukraine, but they were not so geographically confined. Damaging impacts were reported in Germany, Italy, the United Kingdom, Australia, and elsewhere. One of the victims was the Heritage Valley Health System in Pittsburgh, Pennsylvania. Earlier this year, Russia's cyber-attack against satellite company Viasat disrupted critical infrastructure well beyond Ukraine's borders.

We face a new kind of warfare, no longer constrained by borders or military maneuvers. In fact, we face a very different world than the one our then-new Department of Homeland Security entered in 2003, nearly 20 years ago.

The world today is more interconnected than at any time in DHS's 20-year history. Ubiquitous cutting-edge technologies, economic and political instability, and our globalized economy have erased borders and increasingly bring threats and challenges directly into our communities—to our schools, hospitals, small businesses, local governments, and critical infrastructure. Our homeland security has converged with our broader national security.

Those who wish to harm us exploit the openness that defines our modern world. They do so through trade and investment flows, through the rapidly evolving technologies that connect us, and through information spread around the world by the click of a mouse. "Homeland Security" as we thought of it in the wake of 9/11 – safeguarding the United States against foreign terrorism – today has new meaning.

Russia has a wider range of tools to use against its perceived adversaries than it did 20 years ago, all of which have the capacity to create harm here at home. We know the potential for Russia to execute cyberattacks aimed at undermining our economy and our critical infrastructure, and to execute information influence operations designed to exacerbate societal friction, sow discord, and undermine public trust in government institutions and in our democracy.

These tools are not limited to Russia. China has both the capability and intent to challenge the rule-based international order, leveraging its instruments of national power to undermine the security of our critical infrastructure, to gain access to our technology and data, to assault human rights, and to undercut American workers and businesses.

President Biden's National Security Strategy details the twin national security challenges of our time: countering shared transnational challenges and outcompeting our rivals to shape the international order. As the threats have evolved, the historical distinction between homeland security and national security challenges has blurred and the role of DHS has grown accordingly.

Meeting these challenges requires the skills and capabilities that are core competencies at DHS: robust collaboration with the private sector, academia, and all levels of government to identify solutions to threats as soon as they emerge; strong relationships with law enforcement, emergency responders, and critical infrastructure owners that allow us to quickly deliver preparedness tools; and the authority to enforce our laws at home and around the world. It depends on expertise in areas where DHS is playing a critical role for our federal government: counterterrorism, cybersecurity, climate resilience, combatting transnational criminal organizations, pandemic response, and competition with nation states like China and Russia.

This is in addition to our important work to enforce our immigration laws, secure our borders, counter drug trafficking, and build safe, orderly, and humane immigration processes. And, we are doing so, operating within a system that everyone agrees is broken and that Congress must address now, at a time when we are seeing historic migration throughout the hemisphere and around the world.

DHS is using our skills and expertise to meet the challenges of today's world and prepare for the threats of tomorrow. We are more fit for purpose than at any point in our 20-year history.

I am honored to be here today at CSIS to explain why this is so. I will begin with our National Security Strategy's focus on the need to respond effectively to evolving transnational threats.

First, counterterrorism, which continues to be among the most significant transnational issues.

We are confronted with an increasingly complex and dynamic set of terrorism challenges, both at home and around the world – challenges that require DHS and our state, local, tribal, and territorial partners to continue to evolve our counterterrorism capabilities and expand our capacity to prevent all forms of targeted violence.

The familiar set of terrorism threats tied to known terrorist groups, like ISIS and al-Qa'ida, demands we constantly review and improve upon our use of modern technology, the screening and vetting capabilities of CBP, TSA, and USCIS, and our information sharing practices with partners across the globe. Our Automated Targeting System-Global, for example, is a real-time passenger screening system developed for use by our partner nations to assist international officials in making key security decisions and enforcing their respective laws.

The challenge of Domestic Violent Extremism has emerged as one of the greatest terrorism-related threats to the homeland. Our law enforcement partners have a leading role in responding to this threat, and we at DHS are working to support community efforts to prevent and respond to terrorism and other forms of targeted violence when they occur. Our Department will continue to expand its work in this area and partner with local authorities, with academia and civil society, to increase our collective resilience to all forms of violent extremism.

Today, a country's decision to deploy its navy into an adversary's waters is not just a maritime issue. A country's decision to launch a cyber-attack is not just a cybersecurity issue. When a nation launches a cyber assault, it does so in the context of a broader bilateral relationship. When an individual or a group of individuals engage in malicious cyber activity, they are often given license or haven by a nation state.

Emerging technologies and the proliferation of internet-connected services across all sectors and levels of government give our adversaries access to increasingly sophisticated tools, enhancing the speed and scale of cyber threats to the homeland. With a keystroke, our adversaries can disrupt power or water to a small city, mine troves of Americans' personal data, or steal intellectual property. The means by which we address the myriad of cyber-attacks, which are growing in number and gravity, are linked to our role and responsibilities on the global stage.

This imperative is at the heart of our Joint Cyber Defense Collaborative – the JCDC – a communication channel where our Cybersecurity and Infrastructure Security Agency brings together the federal government and the private sector's top network defenders to distill and disseminate insights for the entire cybersecurity community at home and around the world, before damaging impacts occur.

When incidents do occur, DHS ensures we all have a clear understanding of what happened and the lessons we should take away to make us more resilient in the future. We accomplish this through a collaboration between the U.S. government and the private sector – the Cyber Safety Review Board. The CSRB conducts authoritative fact-finding and makes recommendations to the community in the wake of the biggest cybersecurity incidents.

In this environment, even the smallest organizations stand on the front lines defending against the most sophisticated nation state and non-nation state threats. These organizations, including small businesses critical to supply chains and local governments that administer critical services to their residents, have higher risk profiles.

When it became clear Russia was planning its invasion of Ukraine, we mobilized the private sector to proactively harden its cyber defenses against disruptive Russian retaliatory or spillover cyberattacks through a public awareness campaign called "Shields Up," the largest effort of its kind in history.

When Russia did invade Ukraine earlier this year, President Biden immediately turned to DHS, designating us as the lead federal agency for domestic preparedness and response efforts to ensure national vigilance in preparation for any impacts of the conflict that could touch the homeland. We share threat information broadly and in real time with our public and private sector partners, and we identify and mitigate vulnerabilities faster than we ever have before.

DHS helps organizations of all sizes prioritize their investments in cybersecurity, including through voluntary Cybersecurity Performance Goals that outline the highest-priority baseline measures businesses and critical infrastructure owners can take to protect themselves, with easily understandable criteria such as cost, complexity, and impact.

Transnational threats extend, of course, well beyond the cyber domain. Our enforcement agencies are waging the fight against transnational criminal organizations on an unprecedented scale. Our Coast Guard is addressing the impacts of climate change in the Arctic. FEMA is expanding its international engagements to build greater environmental resilience abroad to forestall migratory and other cascading impacts to the homeland. This and much more.

Earlier I referenced our National Security Strategy's emphasis on the imperative to outcompete our primary nation-state rivals in the effort to shape the international order that we will all live under for decades to come. Our cybersecurity work is obviously a critical element of that effort, particularly when it comes to combatting efforts by nations like China to improperly tilt markets in its favor. There are other ways in which DHS carries out critical work to outcompete our rivals.

Our nation derives immense benefits from its open and innovative economic system. Yet that very openness provides opportunities for adversaries who seek to undermine the security of our critical infrastructure and undercut American workers.

Notably, China exploits our global supply chain interdependencies by employing forced labor regimes, profiting from the vilest abuses of human rights and human dignity. The exploitation of vulnerable people undermines our economic security at home and is an afront to our nation's values.

DHS works with a range of nonprofit, private, and public sector entities in a united approach to eradicate forced labor from our supply chains. These partnerships improve the effectiveness of enforcement efforts, like preventing the importation of violative goods from around the world and implementing the Uyghur Forced Labor Prevention Act, which focuses specifically on atrocities taking place in Xinjiang Province.

Each day, DHS plays a critical role in bringing goods to the U.S. market. CBP inspects produce arriving at the Port of Philadelphia, clothing coming into the Port of Los Angeles, and trucks rolling off vessels in the ports of Baltimore and Newark. ICE stands at the forefront of the United States Government's response to global intellectual property theft and the enforcement of hundreds of international trade laws. We have a legal and moral imperative to ensure that products entering our economy are created fairly, and we must do our part to ensure fair competition and a level playing field.

We also remain vigilant against adversaries that attempt to use targeted investments in U.S. firms as another means to undermine the security of our critical infrastructure, or to gain access to cutting edge technology and sensitive data. We

worked closely with the Treasury Department and the White House on President Biden's recent Executive Order on the Committee on Foreign Investment in the United States, which will sharpen our efforts to protect our economy and enhance our focus on investments that impact supply chain resilience, technological leadership, cybersecurity, and sensitive personal data.

DHS, which has played a leading role on CFIUS for the past two decades, is now working with our interagency partners to implement this Order, with a particular focus on ensuring robust and resilient supply chains, implementing the lessons learned from the COVID pandemic. While the acquisition of one small U.S. company by a Chinese company may not pose outsized national security risks, successive small investments across the sector could give China a foothold to exploit and appropriate key technology and intellectual property.

Increasing our international engagement is also a critical part of addressing the global challenges that affect us at home. As new spheres of global competition emerge – like we are seeing in the Indo-Pacific, for example – the capabilities of our Coast Guard in enforcing our laws and maintaining our competitive advantage become more vital. Every agency throughout our Department works closely with allies and partners to leverage their capabilities and to advance our homeland and national security. Through multilateral forums such as the G7 and the Five Eyes partnership, we share information and best practices that are helping address transnational threats and counter nation state actors.

We use our law enforcement partnerships around the world to share critical information and build partners' capacity to help identify threats well before they reach our shores.

The threats of today's world impact our communities and daily lives in ways we could not have predicted even 20 years ago, and the skills and expertise we have built at DHS are essential to our national security.

This is not only true for today's threats, however. As we look to the threats of tomorrow, the capabilities we bring to the mission of securing the nation will be more essential than ever.

DHS is doing our part to counter shared transnational challenges and out-compete our rivals to shape the international order. The men and women of DHS, who comprise the third-largest workforce in the federal government, are among the finest and most dedicated public servants there are. They are driven by a commitment to keep our country and our communities safe.

They are on the front lines – on land, at sea, in the air, and in cyberspace – and we owe them a debt of gratitude.

Emerging technologies, global competition for technological supremacy, a more complex and fragmented trading environment, future pandemics, and climate change are among the trends that will further propel the Department to the forefront of our national security challenges. Regardless of the target, the actor, and the means, our response will require the full capabilities of the national security enterprise – leveraging all tools of our national power, including the expansive array of authorities, tools, and partnerships that reside within DHS.

Twenty years ago, DHS was created from Congress's bipartisan and collaborative efforts to meet a critical need to ensure the protection of our homeland. It remains the largest reorganization of the national security establishment since 1947, when the National Security Act established the Department of Defense and the rest of the modern national security apparatus.

After its founding, a young Department of Defense faced growing pains. Inter-service rivalries hampered effective procurement, research and development, and planning and evaluation. The resulting operational challenges contributed to failure to adequately address the changing threats the nation faced after World War II.

Congress worked together with civilian and military experts to ensure DOD could better deliver on its mission amidst a new era of challenges, passing the Goldwater-Nichols Act in 1986 to better meet the threats facing our nation.

We have built our homeland security capabilities over the past 20 years with lessons learned from DOD's challenges and growth.

We do not do this alone. As I have said many times, DHS is fundamentally a department of partnerships. Addressing the threats of today and tomorrow requires all of us working together across federal, state, and local governments, the private sector, nonprofits, academia, and indeed, the involvement of every individual. The need for DHS's capabilities and tools will only continue to grow as we confront the threats of tomorrow.

Today our homeland security and national security are inextricably linked. We may not have envisioned the complexity and dynamism of today's threat environment when the Department was established 20 years ago, but it is clear we have never been more fit for the mission before us.

Thank you.

###