WRITTEN TESTIMONY

OF

KIRSTJEN M. NIELSEN
SECRETARY
U.S. DEPARTMENT OF HOMELAND SECURITY

FOR A HEARING ON

"Threats to the Homeland"

BEFORE THE

UNITED STATES SENATE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Wednesday, October 10, 2018

Washington, DC

Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee:

It is a privilege to appear before you today to discuss the Department of Homeland Security's (DHS) crucial missions and how we are implementing a policy of "relentless resilience" to confront worldwide threats.

Let me first say that the men and women of DHS are exceptional and dedicated professionals who are on watch 24 hours-a-day, 365 days-a-year protecting Americans from threats by land, sea, air, and in cyberspace, while also safeguarding our values and promoting our nation's economic prosperity. They work tirelessly to strengthen the safety and security of our nation, and to secure it from persistent and emerging threats, including terrorists, transnational criminal organizations, hostile nation-states, natural disasters, and more.

In recent public remarks, I noted that today's threats are very different now than they were at the time of the Department's creation. Today, I will elaborate on that and describe five major changes in the threat landscape that are requiring us to comprehensively rethink homeland security. I will explain how we are building resilience into everything we do, preparing our frontline defenders to protect America in a new age, and responding to these evolving challenges.

A Dark Cloud

Last month marked an important anniversary: 17 years since the 9/11 attacks. We are now many years from the pivotal moment that gave us a permanent mission, but we have not allowed the passage of time to dull our memories or weaken our resolve. We cannot afford to, especially with new storm clouds forming on the horizon.

In the months prior to 9/11, then-CIA Director George Tenet said that the system was "blinking red." Our intelligence professionals were picking up so-called chatter that signaled danger was coming, yet we did not know when or from where. My colleague Dan Coats, the Director of National Intelligence, recently said the system is "blinking red" once again. His concern relates to our nation's digital infrastructure, and he is right to be alarmed. Our digital lives are in danger like never before.

But the danger goes beyond our networked systems and digital world. We are witnessing historic changes across the entire threat landscape. The balance of power that has characterized the international system for decades has been eroding. America's unipolar position is at risk. Power vacuums are springing up across the globe and are quickly filled by hostile nation-states, terrorists, and transnational criminals. They all share a common goal: they want to disrupt our way of life. Many of them are inciting chaos, instability, and violence.

At the same time, the pace of innovation, our hyper-connectivity, and our digital dependence have opened cracks in our defenses, creating new opportunities and new vectors through which these nefarious actors can strike us. This is a volatile combination. The result is a world where threats are more numerous, more widely distributed, highly networked, increasingly adaptive, and incredibly difficult to root out.

The Resilience Agenda

The Department's policy in the face of growing dangers will not be strategic patience. Instead, we are reasserting leadership, and we are focused on building the strongest homeland security enterprise to date. Our approach begins and ends with one word: resilience.

In our darkest hour on 9/11, we saw real heroism, renewed hope, and *relentless resilience*. Americans pledged not to be intimidated by evil. The Department of Homeland Security was born from that commitment, and this year we marked our 15th anniversary. We have come a long way, but we cannot be prepared for everything. What we can do, however, is instill a "culture of resilience" into our everyday lives. That culture is not just about bouncing back; it is about moving forward, adapting when under attack, and emerging stronger than before.

I am pleased to announce that we will soon release a new DHS strategic plan, or "Resilience Agenda," that will guide our actions in defense of the American people.

Our Resilience Agenda is focused on:

- Leaning in against today's threats while zooming out to prepare for those on the horizon;
- Being adaptive to keep pace with our adversaries;
- Identifying and confronting systemic risk;
- Preparing at the citizen level;
- Building redundancy and resilience into everything; and
- Raising the baseline of our security across the board—and across the world.

Perhaps more important than anything are the partnerships we build. In today's world, dangerous actors are crowd-sourcing chaos, and we must crowd-source our response. That is only possible through deep public, private, and international cooperation. These partnerships are a lifeline for America's security and prosperity.

What Has Changed Since 9/11

I will speak today about the five major shifts in the threat landscape and how we are bringing our Resilience Agenda to bear against them.

First, we must recognize that the "home game" and "away game" are no longer distinct. They are one and the same.

After 9/11, our strategy was to take the fight to enemies abroad so we did not have to fight them here at home. Unfortunately, that is no longer the world we live in. Our enemies do not respect borders are not constrained by geography. Today's threats exist in a borderless – and increasingly digital – world. Accordingly, our operating posture must follow suit.

We must reassert our sovereignty by dismantling transnational threat networks that reach into our country, hardening our physical and virtual boundary defenses, and pushing our security measures outward. Indeed, DHS actions abroad are just as important today as our security operations here at home. We have thousands of personnel forward-deployed who are taking an end-to-end approach to dismantling threat networks. This phenomenon—the merging of the home and away game—magnifies all of the others I will talk about today.

Second, terrorism and transnational crime have spread across the globe at fiber-optic speeds.

After 9/11, we faced a centrally-directed terror threat. Today, the threat can exist virtually anywhere. The U.S. Government is conducting terrorism investigations in every state. Self-radicalized terrorists are appearing across the globe. DHS prevents ten individuals with known or suspected terrorism connections a day from traveling to the United States and posing a potential threat to our homeland, and those are just the ones we know about. Even when the United States and our allies destroy jihadist sanctuaries abroad—and we have decimated the so-called caliphate belonging to the Islamic State of Iraq and Syria (ISIS)—they are still able to hide in virtual safe havens online.

Groups such as ISIS and al Qaeda now direct, finance, and inspire attacks from their smartphones. This allows them to act anytime and anywhere with a network connection. They are turning Twitter followers into terrorist foot soldiers. In so doing, they are promoting do-it-yourself terror by urging followers to adopt a "Bring Your Own Weapon" policy, and to conduct violent acts wherever and whenever is convenient.

DHS takes this threat very seriously. In fact, under this Administration, we have made the most sweeping counterterrorism enhancements at the Department since its creation. We have put in place historic measures to keep terrorists from infiltrating the United States, to stop them from radicalizing and recruiting in our communities, and to prevent them from carrying out attacks.

For instance, last year we announced the first-ever "global information-sharing baseline"—a requirement that every nation in the world share information about terrorists and take action to make it harder for them to travel undetected. The handful of countries that failed to comply now face travel restrictions or other sanctions, which have made America safer. In the year ahead, we will be pressing foreign partners to step up their sharing and efforts to prevent terrorist travel, and we look forward to working with partner governments to make it harder for nefarious actors to evade border security.

We have also implemented the toughest screening and vetting measures in DHS history to help weed out violent extremists. We are conducting deeper background checks on foreign travelers, screening applicants against more intelligence information, using biometrics to confirm identities, and conducting more thorough departure and arrival screening. Before the year ends, we will also open a groundbreaking National Vetting Center that will centralize and standardize U.S. Government screening and vetting activities.

Despite their success with do-it-yourself terror, groups such as ISIS and al Qaeda are still focused on executing major attacks, especially against the aviation sector. DHS has met this threat by putting in place the most significant upgrades to aviation security in a decade. In response to threat intelligence, we required every airport in the world with flights to the United States to implement new "seen and unseen" measures to detect concealed explosives, guard against harmful chemicals, and identify insider threats and suspicious passengers. International flights are now more secure than they have ever been.

Our new counterterrorism measures also include: extensive engagement with the tech sector to make it harder for terrorists to weaponize the web with their propaganda; efforts to protect soft targets nationwide against attack; an overhaul of our "terrorism prevention" programs focused on helping communities spot signs of terror sooner; and much more. Last week, the White House released a bold new counterterrorism strategy that puts our enemies on notice and lays out a path to victory against them.

Criminals are exploiting the same environment as the terrorists in order to build cartel superpowers with sprawling networks. Indeed, a decade ago, transnational criminal organizations (TCOs) were much like the terrorists of the 9/11 era: they were confined to certain geographic areas, with a centralized command-and-control structure, and a more limited focus. Today, they are spreading rapidly, outsourcing their work, diversifying their activities, and cooperating with ever-wider cabals of identity forgers, money-launderers, smugglers, traffickers, drug-runners, and killers. They are not only imbedding their enterprises further in the physical world, they are also selling their illicit wares in the virtual world.

In response, DHS is working alongside our international, federal, state, and local partners to pursue renewed efforts to better counter TCOs. In particular, in the coming months we will step up interagency actions with the goal of taking a more global and comprehensive approach to defeating these threats and dismantling their networks for good.

Third, we are witnessing a resurgence of nation states threats.

DHS has spent many years since 9/11 focused on non-state actors. Nevertheless, our nation-state rivals are increasingly asserting themselves in ways that endanger our homeland. In fact, threats to the United States from foreign adversaries are at the highest levels since the Cold War. Countries such as China, Iran, North Korea, and Russia are willing to use all elements of national power—finance, trade, cyber, espionage, information operations, and more—to undermine the United States, and to advance their own interests.

Even in peacetime, hostile nation states are now taking the fight directly to citizens — attacking their personal electronic devices, compromising essential functions as demonstrated in a cyber attack against Ukraine's power grid, targeting individuals directly as we saw with recent poisonings in the United Kingdom, or seeking to destabilize the heart of democracy they depend on through malicious influence campaigns. As I have said before, this is not a fair fight. Neither private companies nor citizens are equipped to oppose nation-state threats alone. So DHS must forge nationwide partnerships to protect our country and our people.

Top of mind for most Americans is the Russian interference in our 2016 elections. At President Vladimir Putin's direction, Moscow launched a brazen, multi-faceted influence campaign to undermine public faith in our democratic process and distort our presidential election. Although no actual ballots were altered by this campaign, this was a direct attack on our democracy. We should not, cannot, and will not tolerate such attacks, nor let them happen again.

Election security was not a mission envisioned for the Department when it was created, but it is now one of my highest priorities. In the past two years, DHS has worked hand-in-hand with officials in all 50 states and the private sector to make our election infrastructure more secure than ever. We are sharing intelligence nationwide with election officials. We are forward-deploying cyber experts to help states and localities scan and secure their systems. By the midterm elections next month, our network security sensors will be deployed to areas to protect the election infrastructure for more than 90 percent of registered voters.

On Election Day, our teams will be out in full force and hosting a virtual, nationwide "situation room" to monitor activity. Our efforts will also continue well after the midterms, and we will work with our partners nationwide to make their systems and processes even more secure. Today, I am calling on every state in the Union to ensure that by the 2020 election, they have redundant, auditable election systems. The best way to do that is with a physical paper trail and effective audits so that Americans can be confident that—no matter what—their vote is counted and counted correctly.

DHS is also undertaking new efforts in partnership with the FBI, the intelligence community, and others to counter foreign influence through close industry engagement and foreign partnerships. Several weeks ago, I helped secure a commitment from our "Five Eyes" partners—Australia, Canada, New Zealand, and the United Kingdom—to collaborate more closely to block meddling in our democracies. More broadly, I have directed a shift from a "counterterrorism" posture at DHS to a wider "counter-threats" posture to ensure we are doing everything possible to guard against nation-state interference. We are overhauling our crisis response teams and advisory boards, realigning our intelligence enterprise into new "mission centers," and taking steps to prevent adversaries from infiltrating U.S. companies and critical industries.

Fourth, cyber attacks now exceed the risk of physical attacks.

Terrorists, criminals, and foreign adversaries continue to threaten the physical security of our people. However cyberspace is now the most active battlefield, and the attack surface extends into almost every American home. A Cybersecurity Ventures report estimates that by 2021, cybercrime damage will hit $6 trillion annually. To put that in perspective, that is equivalent to almost ten percent of the world economy.

It is not just cybercrime we are worried about. Foreign adversaries are working to build the capabilities to attack financial systems, knock out critical services, take down vital networks, and lock down or alter data—calling into question its availability and integrity. Such attacks can spread well beyond their intended targets and have unforeseeable, cascading consequences. This is the viral spread of volatile malware. Indeed, we have moved past the "epidemic" stage and are now at a "pandemic" stage—a worldwide outbreak of cyber attacks and cyber vulnerabilities.

We saw it last year when both Russia and North Korea unleashed destructive code that spread across the world, causing untold billions in damage.

More than 30 nation-states now have cyber-attack capabilities, and sophisticated digital toolkits are spreading rapidly. DHS was founded fifteen years ago to prevent another 9/11, but I believe an attack of that magnitude today is now more likely to reach us online. Virtually everyone and everything is a target, including individuals, industries, infrastructure, institutions, and our international interests.

In response, earlier this year, DHS released a new cyber strategy that outlines how we are changing the way we do business. Above all, it highlights how we will identify and confront systemic risk, moving away from a focus on the protection of specific assets or systems. In July, DHS hosted the first-ever National Cybersecurity Summit, where we brought together top CEOs and cyber minds to discuss these issues. We agreed that we cannot afford to defend ourselves in silos. If we prepare individually, we will fail collectively. We must move from endemic vulnerabilities to system-wide endemic resilience.

To support this strategy, I announced the launch of the DHS National Risk Management Center, which will serve as a central hub for government and private sector partners to share information and better secure the digital ecosystem. Together we will identify single points of failure, concentrated dependencies, and cross-cutting underlying functions that make us vulnerable. We are also driving forward ambitious supply chain security efforts to identify upstream weaknesses before they have downstream consequences.

DHS is working with our partners throughout the Administration to hold cyber attackers accountable. We will no longer tolerate the theft of our data, nor stand by as our networks are penetrated, exploited, or held hostage. We will respond decisively. The United States has a full spectrum of options—some seen, others unseen—and we are already using them to call out cyber adversaries, to hold them to account, and to deter future malicious actions.

This Administration is replacing complacency with consequences and replacing nations' deniability with accountability. However, DHS was not built for a digital pandemic. Our cybersecurity arm—the National Protection and Programs Directorate—needs to be authorized in law and transformed into a full-fledged operational agency. Today, I ask Congress to pass legislation immediately, and absolutely before the year's end, to make this a reality. I thank Senators on this Committee for their hard work in helping us move to establish the Cybersecurity and Infrastructure Security Agency, and for the Senate's recent action to advance that legislation.

Fifth and finally, emerging threats are outpacing our defenses.

Unmanned aerial systems, often referred to as drones, are a prime example. Terrorists are using drones on the battlefield to surveil and to destroy; drug smugglers are using them to monitor border patrol officers so they can slip into America undetected; and criminals are using them to spy on sensitive facilities. The threat is real, and they can be used for a wide array of nefarious purposes.

Unfortunately, outdated laws have prevented us from setting up the sophisticated countermeasures we need to protect significant national events, federal facilities, and other potential targets from an airborne menace. DHS has lacked the clear legal authority to track and identify dangerous drones—and to neutralize them effectively if they are determined to be a threat. Furthermore, we have not been able to test many of the crucial countermeasures we need in real-world environments where the risks exist.

Today I am pleased to offer our gratitude to this Committee for helping us secure these authorities in the *FAA Reauthorization Act of 2018* to get ahead of this challenge. The President signed this bill into law last week, and it will give us the ability to better protect Americans against unmanned aerial threats. We have already begin planning in earnest for how to best deploy these authorities and defensive technologies to defend the United States against this emerging danger.

Our professionals at DHS are also concerned about weapons of mass destruction. For instance, terrorists and nation-states continue to explore the use of chemical and biological weapons to conduct attacks. We have seen Russian intelligence operatives poison civilians in the United Kingdom using a deadly military-grade nerve agent, the brutal Assad regime use chlorine and sarin gas to attack their own people, and ISIS deploy chemical weapons on the battlefield. We remain concerned that terrorist groups are seeking to use such capabilities in plots outside of conflict zones.

DHS is taking these threats seriously. Last December, I formed the DHS Countering Weapons of Mass Destruction (CWMD) Office. It was one of the most important DHS reorganizations in years and has already helped us better protect the American people. Although CWMD has broad authorities to guard against radiological and nuclear dangers, the office does not have the same comprehensive authorities to defend against chemical and biological threats. However, thanks to the leadership of this Committee and the House Homeland Security Committee, we are close to strengthening our CWMD office by empowering it with the authorities it needs. The House passed this legislation, and we urgently need the full Senate to do the same. The Department cannot adequately fulfill its missions in the chemical and biological spaces without these crucial authorities being provided this year.

Closing

I cannot tell you how proud I am to lead the 240,000 men and women of the Department of Homeland Security. Every day, they roll up their sleeves and go to work to build a better and safer America. They enforce the laws passed by Congress. They believe in accountability. And they are relentlessly resilient.

Whether it is a FEMA employee supporting the response to fires and floods …or an ICE agent taking a murderer off the streets…or a Coast Guard lieutenant seizing drugs near our shores…or a CBP officer stopping a terrorist trying to enter the country…or a TSA agent working to keep explosives off of airplanes…or a USCIS officer helping a family of refugees find a safer life in our country…or a Secret Service agent taking down a fraud scheme...or a cyber analyst sharing threat indicators to stop a digital heist...or a FLETC instructor providing much needed training to

law enforcement officers from communities across America…or the many, many other employees who work to protect our homeland. They all deserve our respect and gratitude. As do their families—for when one serves at DHS, his or her family serves too.

I can tell you firsthand these patriots have thwarted real plots, real threats, and real danger to our people in just the ten months I have been on the job. I will continue to work with Congress to make sure we are doing everything possible to support them so that, with honor and integrity, they can continue to safeguard the American people, our homeland, and our values.

I want to thank you, Chairman Johnson, Ranking Member McCaskill, distinguished Members, and staff for the support you have shown the Department, and the work undertaken by this Committee to ensure DHS has what it needs to adapt to the changing threat environment.

Thank you.