STATEMENT FOR THE RECORD
BY THE HONORABLE MICHAEL CHERTOFF
CO-FOUNDER AND EXECUTIVE CHAIRMAN OF THE CHERTOFF GROUP
AND FORMER SECRETARY OF THE
U.S. DEPARTMENT OF HOMELAND SECURITY
FOR THE UNITED STATES SENATE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENT AFFAIRS
SEPTEMBER 9, 2019

I want to thank Chairman Johnson, Senator Peters and members of the Committee for inviting me to participate in this special occasion as we come together with the same unity of purpose that we had18 years ago, reflect upon the tragic events that occurred on September 11, 2001, and what has been done to prevent such events from occurring again.

I would also like to take this opportunity to recognize my fellow secretaries sitting with me on this panel today. In decidedly partisan times, it is reassuring that we are able to come together to reflect on the collective work that all of us have done to protect the safety and security of the American people. Even today, after our government service, we remain committed to the goal of securing a safe future for our country and our citizens.

I want to state clearly that I am submitting this Statement in my personal capacity, although, for the record, I am Co-Founder and Executive Chairman of The Chertoff Group, a global security and risk management company that provides strategic advisory services on a wide range of security matters. Additionally, I am Senior of Counsel to the law firm of Covington and Burling, LLP, and I am Chairman of the Board of Freedom House.

Following the attacks on September 11, 2001, the United States worked steadfastly to confront the national security threats that terrorism posed to this country. We worked with international partners to disrupt and dismantle terrorist plots overseas before they reached our shores and built effective capabilities to better manage risk here at home. Over time, I believe we have significantly improved our nation's capabilities to protect our homeland, not only from large scale terrorist attacks such as those we witnessed on 9/11, but other threats facing our nation as well. These investments and improved capabilities include:

- Enhanced screening of people and cargo traveling to the United States by air, sea, and land;
- Improved information sharing abilities across law enforcement agencies within the U.S. as well as with international partners;
- Stronger protection measures and partnerships for our nation's critical infrastructure and key resources; and
- A greater culture of preparedness and resilience across our local communities as well as the nation as a whole.

These investments will continue to be important as we review, assess, and renew our approach to risk -- cyber or physical, or otherwise -- and the investments necessary to protect our nation and its citizens.

That said, today we face a variety of threats and must consider what type of capabilities are needed to manage these risks and where these threats are likely to evolve in the future.

Terrorism

According to the Director of National Intelligence's 2019 Worldwide Threat Assessment, terrorism continues to be a top threat to the U.S. and partner interests worldwide. Despite progress made on this front, there remains a constant and persistent desire to strike the U.S. as well as our interests and people overseas. The large scale, high visibility, high impact attacks like September 11th are still a risk. However, we have taken great steps to reduce this risk, or what I call Terrorism 1.0. We must be careful that to the extent the U.S. considers the withdrawal of troops from Afghanistan, we also work to ensure that the progress made to reduce this risk today is not reversed by enabling terrorists or armed insurgents to rebuild training camps or testing labs which can enhance their ability to plan, prepare, train and ultimately, bring harm to the U.S. and our allies.

As we reduced the ability for terrorists to carry out the large scale Terrorism 1.0 style attacks, we saw an increase in smaller groups carrying out attacks … such as the Mumbai attack in 2008. I refer to these types of attacks as Terrorism 2.0. These attacks are led by smaller groups and often require less resources to carry out. They often use easily-available resources, such as firearms,

and choose multiple soft targets with the primary goal of killing and terrorizing the innocent in the name of their cause.

The terrorists now have also moved to what I call "inspired terrorism," or Terrorism 3.0, where it is not necessarily attacks by well-trained people or well-planned terror events, but lone action by individuals who become inspired on the Internet and simply pick up a gun or the keys to a car or build a homemade bomb and kill somebody. That is what we are seeing in terms of white supremacists "inspired" to carry out an attack on others. But we have also seen that with jihadis in places like Europe for example, and it is part of the same phenomenon.

The increase in domestic terrorist incidents has also been largely prompted by growing networks of individuals associated with terror organizations or sympathetic to their cause. These networks, largely existing online, incite people to carry out acts of violence, both explicitly and implicitly. While attacks connected to such networks are generally smaller in scale and less coordinated, they achieve the perpetrator's desired goal of using violence to intimidate a particular faith group, ethnic group, or community. This intimidation has an effect not only on the particular geographic region where it occurs, but also successfully undermines our nation's sense of security. These small-scale attacks have multiplied over time and now outpace international jihadist attacks in their frequency.

While DHS has made progress in enhancing the ability of law enforcement to communicate across agencies, continued investment in multi agency fusion centers will be vital to combating the threat of domestic terrorism. When trying to detect these lone, inspired individuals, you cannot rely on the same capabilities with regard to intelligence resources as you do with large scale attacks. Often, these types of individuals or potential events are very local, and you have to deal with local authorities and local friends and local family. We have to ask them when they see somebody who is beginning to go off the rails, they need to communicate with the people in government or the FBI, or the police and say, somebody is now talking about doing something or beginning to act in a way that suggests they might be a threat. And we need to ensure these local authorities, including law enforcement, are training to detect and investigate this type of activity. And, as part of this strategy, we need to support community and private groups that can de-program or "off-ramp" individuals who are beginning to veer into violence, but have not yet taken steps to violate the law.

Further, as we've witnessed, the vast majority of attackers in recent domestic terrorist incidents have used the internet to consume and post extremist views and connect with a network that shares their ideology. By effectively utilizing open-source intelligence we increase our ability to circumvent a planned attack as well as study the online behavior of those that espouse hateful philosophies. We must also continue to work with major content and social media platforms to identify and investigate potential threats.

Cyber

The world has changed tremendously in the last 18 years. We have never been more interconnected; information moves faster, and perceived distances are smaller. While the convenience of these technological developments should not be discounted, we must recognize that we have developed a reliance. With this reliance comes risk.

Currently, there is a battle going on within our computer networks against a complex array of adversarial actors. The bombardment of our government networks and critical infrastructure is constant. We are exposed to a wide range of threats and actors. This not only includes those from well-funded nation states and global criminal organizations, but increasingly from individual actors, some truly independent, some acting on instructions from nation-state leaders, and others acting in concert based on a shared ideology.

We see nation states using the very technology that brings us together to drive us apart and undermine trust in our political systems. We see hacker groups manipulating DNS infrastructure to redirect government agency computers to hacker-controlled servers. We see a new network, 5G, being developed predominantly by companies based outside the United States. This technology offers incredible opportunities, but also creates risks that must be managed.

In this environment, there are a number of areas of activity that I would highlight as vital to allowing us to address the most pressing threats.

First, in the area of election security, the work of DHS' Cyber and Infrastructure Security Agency or CISA is making progress in helping to enhance cyber and physical infrastructure security. In particular when it comes to election security, CISA has helped provide information to state and local election officials to help them defend their infrastructure and partnered to share cybersecurity risk information and we see action being taken. In 2016, less than 30% of election

infrastructure was protected by intrusion detection systems. By the last midterms, coverage was up to 90%.[1] This is a great accomplishment, but more must be done. We need to allocate more money and resources for CISA to continue its mission and work with states and localities in need of further assistance. We also need to act to deter foreign adversaries from trying to affect our elections.

Second, I believe that we need to foster growth within the National Technology Industrial Base. During the Cold War, the Defense Industrial Act was effective at maintaining the United States' industrial advantage, but now its limitations are starting to show. Globalization has made the production of certain technologies—computer chips for instance—prohibitively expensive in the United States. While Congress' amendment to the Defense Industrial Act to include dual-use technologies was a step in the right direction, there is still much to be done.[2] We must "recognize these changed circumstances and then reconstruct legal and policy standards."[3]

Third, supply chain vulnerabilities, both digital and physical, are of increasing concern. The U.S. government must continue to prohibit federal agencies from using hardware and software from companies that pose a national security risk. The U.S. government has already done this with the prohibitions of Russia's Kaspersky and China's Huawei. We must continue to take action to protect our critical infrastructure supply chain. Our electrical grid, banking system, and water supply are critical aspects of our economic and national security, and their vulnerabilities must be secured.

Fourth, the U.S. government must focus on cultivating its relationship with our allies and with the private sector, which plays a paramount role in the National Technology Industrial Base. We have entered an era where nearly every technology we encounter is effectively "dual-use," that is, a technology that has civilian, government, and military applications. DHS, the intelligence community, and the Department of Defense are all reliant on technologies developed in the private sector and supply chains that provide equipment to both the commercial sector and

---

[1] Chris Krebs, October 11, 2018, "Securing the Election: Are We Ready for the Midterms?." Podcast audio, *Insights & Intelligence*, The Chertoff Group, October 11, 2018, https://podcasts.apple.com/us/podcast/011-securing-the-election-are-we-ready-for-the-midterms/id1434604274?i=1000421867415&mt=2.

[2] Michael Chertoff and Mike McConnell, "Former Heads of DHS and NSA Explain How the U.S. Can Keep Huawei at Bay," *CNBC,* July 11, 2019, https://www.cnbc.com/2019/07/11/chertoff-mcconnell-us-needs-to-have-more-allies-to-bypass-huawei.html.

[3] Michael Chertoff, *Exploding Data* (New York, Atlantic Monthly Press, 2018), 16.

government. In this environment it is paramount that our leaders work closely with leading American technology companies, working to ensure that their products remain cutting edge and have the security needed to be used in our homes, businesses, power plants, and government buildings.

New Threats

Finally, we must not become complacent and/or repeat the failures of the past by not using our imagination. We must be actively thinking, considering and imagining potential threats to nation's peace and prosperity. Some of these are already evolving today with evidence pointing to the growing impact that climate change is having on the natural disasters that face our country. They are increasing not only in frequency, but in intensity and economic impact. We must look at the likely impacts that climate change will have on our ability to withstand and respond to natural disasters. The most effective investment is in risk mitigation, which the National Institute of Building Sciences recently found to offer $6 in savings for every $1 invested in disaster mitigation.[4] As such, we should continue to make investments consistent with the National Mitigation Investment Strategy, working to reduce risk through strategic investments in preventative and preparedness measures, such as updated building codes, ease access to information, and provide additional funding for mitigation activities.[5] We also need to allow for and fund further research into the likely impacts of climate change on other important national and economic security issues including the potential for mass migration, the shifting or sudden scarcity of important resources and/or the potential opportunity for control or conflict in changing environments such as the Arctic.

Conclusion

I want to thank you for this Committee's continued focus on our nation's homeland security and the opportunity to share my views today. I also want to publicly thank the thousands of men and

---

[4] "National Institute of Building Sciences Issues New Report on the Value of Mitigation," *National Institute of Building Sciences*, January 11, 2018, https://www.nibs.org/news/381874/National-Institute-of-Building-Sciences-Issues-New-Report-on-the-Value-of-Mitigation.htm.

[5] "National Mitigation investment Strategy," *Mitigation Framework Leadership Group, Department of Homeland Security*, August 2019, https://www.fema.gov/media-library-data/1565706308412-19739d7deeca639415cc76c681cee531/NationalMitigationInvestmentStrategy.pdf.

women who continue to serve this mission daily as part of the Department of Homeland Security. I had the opportunity to observe their tireless dedication to our nation's safety and security and the service they perform daily to prevent future terrorist attacks from occurring here at home.