Statement of Frank J. Cilluffo

Director, McCrary Institute for Cyber and Critical Infrastructure Security

Auburn University

Before the House Permanent Select Committee on Intelligence

25 Years After 9/11: Confronting the Next Generation of Threats

July 21, 2026

I. Twenty-Five Years Later

Chairman Crawford, Ranking Member Himes, and distinguished Members of the Committee, thank you for the opportunity to appear before you today as part of the Committee's important examination of the evolving threats facing the United States twenty-five years after the terrorist attacks of September 11, 2001. I appreciate the opportunity to discuss how the strategic environment has changed, what those changes mean for the security of the homeland, and how the United States should posture itself for the challenges ahead.

As we approach the twenty-fifth anniversary of September 11th, we do so first with solemn remembrance. We honor the 2,977 innocent lives lost that day, the families forever changed by their absence, and the extraordinary courage of the first responders, intelligence professionals, military personnel, law enforcement officers, and countless public servants who answered the Nation's call in the days, months, and years that followed. Their service fundamentally reshaped how America thinks about homeland security, and the institutions they built continue to protect our Nation today.

For many Americans, September 11th remains a defining national memory. For some of us, it also remains a defining professional responsibility. I was privileged to play a small role in the United States Government's response during the months and years that followed. That experience reinforced a lesson that has guided much of my career since: perhaps the greatest tribute we can pay to the generation that answered the call after September 11th is not simply to preserve what they built, but to ensure it continues to evolve as the threat itself evolves.

September 11th represented not simply a national tragedy, but a strategic inflection point. The attacks fundamentally altered America's understanding of homeland security and demonstrated that geographic distance no longer guaranteed strategic protection. In response, the United States undertook one of the most significant reorganizations of the federal government since the National Security Act of 1947. The creation of the Department of Homeland Security, the establishment of the Office of the Director of National Intelligence and the National Counterterrorism Center, strengthened intelligence integration, expanded information sharing, deeper collaboration among federal, state, local, tribal, territorial, and private-sector partners, and closer cooperation with our closest allies, particularly our Five Eyes partners, collectively transformed the Nation's ability to identify threats before they matured into catastrophe.

Those reforms unquestionably made America safer. More importantly, they demonstrated something enduring about the American character. Faced with a fundamentally different threat environment, the United States proved willing to challenge long-held assumptions, reorganize institutions, forge new partnerships, and adapt. That willingness to evolve may ultimately prove the most important lesson of the post-September 11th era.

The question before us today is whether we remain equally willing to do so again.

Today's threats look fundamentally different. Not because the danger has diminished, but because our competitors have adapted. The threat spectrum now comes in various shapes, sizes, and forms. Twenty-five years ago, terrorists weaponized commercial aviation. Today, America's principal adversaries increasingly seek to weaponize the very systems upon which modern society depends. While the methods have changed, the underlying objective has not. Our adversaries continue to seek strategic advantage by weakening American power, limiting our freedom of action, and undermining public confidence. Increasingly, however, they pursue those objectives through cyber operations, attacks against critical infrastructure, economic coercion, influence campaigns, and other forms of gray-zone competition deliberately designed to remain below the threshold of conventional armed conflict.

That distinction should fundamentally shape how we think about homeland security over the next twenty-five years. The objective is no longer simply inflicting immediate physical destruction. Increasingly, it is achieving persistent strategic leverage by exploiting America's dependence upon interconnected infrastructure, advanced technologies, and globally integrated supply chains. History reminds us that America's competitors continuously study our strengths, identify our vulnerabilities, and adapt their own strategies accordingly. As the United States invested heavily in preventing another catastrophic terrorist attack, those same competitors increasingly developed methods of coercion capable of imposing strategic costs while avoiding the traditional thresholds associated with armed conflict.

Our success over the past twenty-five years should therefore give us confidence, but never complacency. The extraordinary efforts of the Intelligence Community, the Department of Homeland Security, the Federal Bureau of Investigation, the U.S. military, state and local law enforcement, and countless private-sector partners significantly reduced the likelihood of another catastrophic terrorist attack on the scale of September 11th. Terrorism remains an enduring threat that demands sustained vigilance. Yet the defining characteristic of today's strategic environment is not that terrorism has disappeared. It is that new threats have accumulated alongside it. Policymakers must now simultaneously sustain hard-earned counterterrorism gains while competing with sophisticated nation-state adversaries employing cyber operations, economic coercion, influence campaigns, espionage, technological competition, and other gray-zone activities to achieve strategic objectives without triggering conventional military conflict.

One lesson from the past twenty-five years is particularly clear. **We cannot prepare for tomorrow's threats using frameworks designed for yesterday's conflicts. We cannot afford to march into the future looking through the rear-view mirror.** Instead, homeland security must continue evolving—building upon the extraordinary successes achieved since September 11th while adapting to a strategic environment increasingly defined by great-power competition. The evidence points toward a single strategic conclusion:

the homeland itself has become a contested operating environment. Recognizing that reality is the essential first step. The next is ensuring that our strategy, institutions, doctrine, and operational capabilities evolve as rapidly as the threats confronting them.

It is within that broader strategic context that the changing character of cyber conflict—and its implications for the homeland—should be understood.

The Changing Character of Strategic Competition

For much of the twentieth century, Americans viewed the homeland as a sanctuary from great-power competition. Geography provided strategic depth. Military operations were expected to occur overseas while the homeland generated the economic, industrial, technological, and military capacity necessary to sustain them. That assumption no longer holds.

America's principal competitors increasingly seek strategic advantage not by defeating the United States in conventional battle, but by holding at risk the systems that generate, sustain, and project American power. Energy, communications, transportation, logistics, financial services, cloud infrastructure, space-based capabilities, and other elements of critical infrastructure have become integral not only to our economy, but also to our military readiness and our ability to project power abroad. The distinction between homeland security and national security has therefore become increasingly artificial. Defending civilian critical infrastructure is no longer simply an economic imperative; it has become an essential component of national defense.

This transformation reflects a broader evolution in the character of strategic competition. Rather than seeking decisive battlefield victories, our competitors increasingly pursue cumulative strategic advantage through campaigns that remain below the threshold of conventional armed conflict. Cyber operations, economic coercion, espionage, technological competition, influence operations, supply chain manipulation, and other gray-zone activities are not isolated lines of effort. They are mutually reinforcing components of long-term campaigns designed to shape the strategic environment in their favor while avoiding the costs and risks of direct military confrontation.

One of our enduring challenges is that we often analyze these threats through the organizational structures we have created to address them. Cyber belongs to one office, counterintelligence to another, critical infrastructure to another, influence operations to another, and emerging technologies to yet another. Our adversaries recognize no such distinctions. They synchronize cyber operations, espionage, economic coercion, influence activities, technological competition, space capabilities, autonomous systems, and increasingly artificial intelligence into integrated campaigns designed to achieve strategic effect. Understanding the contemporary threat environment therefore requires moving beyond individual incidents and viewing adversary behavior as coordinated campaigns that integrate multiple instruments of national power in pursuit of strategic objectives.

Our adversaries get a vote, and they are not constrained by our organizational charts. Neither should our thinking be.

Viewed individually, many of these activities appear manageable. Viewed collectively, however, they constitute strategic warning indicators that deserve far greater attention from policymakers.

No example better illustrates that evolution than the cyber campaigns conducted by the People's Republic of China against the United States over the past decade. These campaigns should not be viewed as isolated incidents or disconnected episodes. Rather, they reveal a deliberate evolution in how America's principal competitors seek to achieve strategic advantage with the hopes of avoiding military retribution. Campaigns associated with Volt Typhoon, Flax Typhoon, Salt Typhoon, and others demonstrate an increasingly integrated strategy that extends well beyond traditional espionage. Although each differs in its immediate objectives and methods, collectively they reveal an adversary seeking persistent access to the systems upon which the United States depends.

Among these campaigns, Volt Typhoon is particularly significant because it illustrates how cyber operations have evolved beyond intelligence collection toward operational preparation of the battlefield. Rather than simply collecting information, China appears to have deliberately positioned itself within elements of U.S. critical infrastructure to create options for disruption or degradation during a future crisis or conflict. This is no longer merely intelligence collection. It is the deliberate positioning of capabilities intended to create strategic advantage before conflict begins. This is not simply a cybersecurity challenge. It is increasingly a counterintelligence challenge that requires us to identify, understand, and disrupt hostile access before it can be translated into strategic effect. The traditional distinction between exploitation and attack is becoming increasingly thin. In many cases, the technical difference is minimal; what separates the two is not capability but intent. Once an adversary has established persistent access to critical systems, the transition from intelligence collection to disruption can occur whenever strategic circumstances dictate. In combination, these campaigns are best understood not as isolated cyber incidents, but as elements of a sustained strategic campaign designed to create options for coercion, disruption, and military advantage during periods of heightened tension or conflict.

The implications extend far beyond cybersecurity. Civilian infrastructure increasingly underpins military effectiveness. Transportation networks move forces and equipment. Energy systems power military installations and industrial production. Commercial communications enable command, control, and logistics. Cloud infrastructure supports both government and private-sector operations. Ports, rail systems, and digital supply chains sustain military mobility and the Defense Industrial Base. An attack against these systems may not directly target military forces, yet it can significantly impede America's ability to mobilize, reinforce allies, sustain combat operations, and project power abroad.

Protecting civilian critical infrastructure is therefore inseparable from preserving the Nation's military readiness and long-term strategic advantage.

The same strategic logic extends beyond cyberspace. Space-based capabilities have become indispensable to emergency response, transportation, communications, financial services, agriculture, precision navigation, intelligence collection, and military operations. The rapid evolution of unmanned aircraft systems presents another illustration of how technologies once associated primarily with overseas battlefields are increasingly reshaping homeland security. The conflict in Ukraine has demonstrated that inexpensive, commercially available systems—employed individually or in coordinated swarms—can conduct surveillance, collect intelligence, strike targets with remarkable precision, overwhelm traditional defenses, and impose disproportionate operational and economic costs. Equally important, the conflict has demonstrated the extraordinary pace at which these capabilities are evolving, often adapting in weeks or months rather than years. The lesson is not simply that drones are becoming more capable. It is that precision capabilities once largely reserved for advanced militaries are becoming increasingly accessible to state and non-state actors alike.

The United States should view these developments not simply as lessons from a distant conflict, but as previews of homeland security challenges that are increasingly likely to emerge here at home. In many respects, today's battlefields are previews of movies coming soon to a theater near you—not overseas, but potentially at a military installation, major public event, energy facility, transportation hub, or Main Street somewhere in America. Much as cyber has erased the traditional distinction between foreign and domestic threats, inexpensive autonomous systems are increasingly eroding the historical separation between overseas battlefields and homeland security. As unmanned systems become cheaper, more autonomous, and increasingly enabled by artificial intelligence, protecting critical infrastructure, public venues, military installations, and the American people will require a far more integrated approach to detection, attribution, authorities, and layered defense than has traditionally existed.

Artificial intelligence will accelerate each of these trends. It will compress decision timelines, increase the scale and speed of cyber operations, enhance intelligence collection and analysis, improve autonomous systems, amplify influence campaigns, and lower barriers to sophisticated capabilities. The rapid development of AI raises distinct policy questions, but it should not be viewed as a separate challenge. Rather, it is an accelerator of the broader strategic trends reshaping homeland security.

Recent public discussion surrounding advanced AI systems such as Mythos illustrates both the strengths and the responsibilities of an open society. It also invites an important strategic question. Had Beijing developed a comparable capability first, would there have been a public debate? Would there have been a press conference? Or would we have discovered it only after it had already been incorporated into cyber operations, intelligence collection, or operational planning directed against the United States and its allies?

That distinction is more than cultural. It reflects fundamentally different approaches to strategic competition and should inform how democratic societies preserve technological advantage while competing against adversaries who operate under very different assumptions.

Together, cyber operations, space capabilities, artificial intelligence, autonomous systems, and other emerging technologies reinforce the same strategic reality: the homeland itself has become an increasingly contested operating environment. Recognizing that reality fundamentally changes how we should define success.

For many years, cybersecurity has emphasized preventing intrusions wherever possible. Strong defenses remain indispensable, but they are no longer sufficient by themselves. Sophisticated adversaries will, at times, penetrate even well-defended networks. The more consequential question is whether they can achieve their strategic objectives once they do. America's objective must therefore extend beyond preventing compromise to ensuring that the Nation can continue governing, communicating, mobilizing military forces, delivering essential services, and projecting power despite persistent disruption. In short, **America must be able to operate through compromise.**

That represents a profound shift in thinking. Success can no longer be measured solely by whether an adversary gains access to a network. Increasingly, it must be measured by whether the Nation continues to function despite that intrusion. Preparedness for the next twenty-five years should therefore emphasize continuity of government, continuity of military operations, continuity of critical infrastructure, realistic exercises under degraded conditions, and resilience measured by operational outcomes rather than technical compliance alone. Whether the contested domain is cyberspace, outer space, or the homeland itself, the strategic logic is remarkably similar: America's competitors increasingly seek to hold at risk the systems that generate, sustain, and project American national power while avoiding conventional military conflict.

The next phase of homeland security should not be defined by abandoning the lessons of the past twenty-five years, but by applying them to a strategic environment that has changed fundamentally. The institutions, partnerships, and capabilities developed after September 11th remain indispensable. The challenge is ensuring that they continue to evolve for an era in which the homeland is contested, adversaries operate persistently below the threshold of conventional conflict, and the systems that sustain American society are increasingly inseparable from those that generate and project American power. America must preserve the hard-earned gains of the post-9/11 era while adapting its strategies, doctrine, authorities, partnerships, and operational concepts to meet a wider and more complex threat environment.

The recently released National Cyber Strategy provides an important framework for that evolution and rightly recognizes the need for a more proactive posture in cyberspace. The challenge before us is no longer developing strategy. It is translating strategy into

operational capability. Strategic objectives must be converted into doctrine, operational concepts, planning, training, exercises, appropriate authorities, and measurable outcomes. Strategies matter, but their value is ultimately determined by whether they enable the United States to preserve the initiative, shape the operating environment, strengthen deterrence, impose meaningful costs where necessary, and prevent adversaries from achieving strategic effects.

That imperative is particularly important in cyberspace. The United States has made substantial progress in strengthening network defense, improving incident response, and increasing resilience across government and industry. Those efforts remain essential, but defense alone is insufficient against sophisticated competitors conducting persistent campaigns designed to accumulate advantage over time. We cannot firewall our way out of this challenge. Defending forward, persistent engagement, and the appropriate use of offensive cyber capabilities should be understood not as substitutes for strong defense, but as complementary elements of a broader national strategy. The objective is not to conduct offensive cyber operations for their own sake, nor merely to win individual cyber engagements. It is to shape adversary decision-making, preserve freedom of action, impose costs before malicious activity produces strategic consequences, and strengthen America's position in the broader competition.

The United States must also move beyond an operating model centered primarily on information sharing. Information sharing remains indispensable, and the progress made across government, industry, and among trusted allies should be preserved. The demands of persistent strategic competition, however, require operational collaboration: government agencies, the Intelligence Community, the Department of Defense, state and local authorities, private-sector owners and operators, and close allies planning, exercising, and acting together before crises occur. Success should be measured not by the volume of information exchanged, but by the operational outcomes achieved -- threats identified earlier, vulnerabilities reduced, essential services sustained, adversary campaigns disrupted, and national freedom of action preserved.

This requirement is especially important because much of the infrastructure upon which American national power depends is privately owned and operated. Military mobilization, logistics, communications, transportation, cloud services, energy, industrial production, and the Defense Industrial Base all rely upon civilian systems and commercial partners. Protecting that infrastructure is therefore not solely an economic or public-safety responsibility; it is integral to military readiness and national defense. The United States must develop stronger mechanisms for trusted planning, realistic exercises, rapid operational coordination, and sustained partnership with the companies that own, operate, and increasingly innovate the capabilities upon which the Nation depends.

The same principle should guide cooperation with allies. One of America's greatest strategic advantages is its network of trusted partners, particularly the Five Eyes and our closest NATO and bilateral allies. Our adversaries often seek to exploit seams between

countries, agencies, sectors, and authorities. We should respond by deepening the trusted relationships that permit earlier warning, shared situational awareness, coordinated action, and collective resilience. The United States should not compete as a collection of institutions or as a nation acting alone. It should compete as the center of an integrated network of allies, public institutions, private-sector partners, universities, and innovators capable of adapting faster than those who seek to challenge us.

America must also redefine resilience for a contested homeland. Sophisticated adversaries will, at times, penetrate even well-defended networks and disrupt systems we depend upon. The decisive question is whether they can translate that access into strategic effect. America must be able to operate through compromise and in degraded environments. Government must continue governing, the military must continue mobilizing and projecting power, critical infrastructure must continue delivering essential services, and the private sector must continue sustaining the economic activity upon which national power depends. This requires continuity planning, realistic exercises, redundancy, rapid recovery, and operational doctrine designed not merely to prevent disruption, but to sustain essential national functions during it.

Artificial intelligence will accelerate nearly every element of this environment. It will increase the speed and scale of cyber operations, compress decision timelines, enhance intelligence collection and analysis, amplify influence campaigns, improve autonomous systems, and lower barriers to sophisticated capabilities. AI should therefore not be treated as a stand-alone policy problem. It is an accelerator of the broader trends reshaping homeland security. The strategic advantage will not necessarily belong to the actor with the most data or the most capable model. It will belong to the actor best able to integrate technology with sound judgment, trusted access, operational discipline, resilient institutions, and clear strategic purpose. Technology changes warfare. It does not replace strategy.

Congress has an indispensable role to play, but the central requirement is not necessarily the creation of another institution or the publication of another strategy. The priority should be ensuring that existing strategies are implemented, authorities are usable, responsibilities are clear, and agencies possess the doctrine, capabilities, workforce, and resources necessary to act. Oversight should emphasize operational outcomes rather than policy outputs. Are threats being identified earlier? Are adversary campaigns being disrupted? Are critical services more capable of operating under pressure? Can military forces deploy and sustain operations in contested conditions? Are agencies looking beyond traditional roles to collaborate in service of the larger strategy? Are government and industry exercising together against realistic scenarios? Are we preserving the Nation’s freedom of action and reducing the strategic leverage available to our adversaries?

The measure of homeland security is no longer simply preventing disruption. It is preserving national power despite disruption. That requires a posture capable of defending where necessary, deterring whenever possible, and, where appropriate, shaping and

compelling adversary behavior before malicious activity produces unacceptable consequences. It also requires a national-security enterprise that is resilient enough to absorb shocks, agile enough to adapt under pressure, and integrated enough to act across institutional, sectoral, and national boundaries.

Twenty-five years ago, the United States confronted a strategic surprise that forced us to rethink how we defended the homeland. The response demonstrated our capacity to adapt with urgency, unity, and purpose. We should draw confidence from that history, but never complacency. Dark clouds are again gathering on the horizon. The threats are different, the technologies are different, and the pace of competition is faster, but our responsibility remains the same. We cannot afford to march into the future looking through the rear-view mirror. If we recognize that the homeland has become a contested operating environment, build the capacity to operate through compromise, translate strategy into operational capability, and preserve the initiative against our adversaries, I am confident the United States will once again rise to the occasion.