Statement of LTG H.R. McMaster (U.S. Army, retired)

Senior Fellow, Hoover Institution, Stanford University

Before The House Permanent Select Committee on Intelligence

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

21 July 2026

H.R. McMaster

Lauriecg@stanford.edu

Chairman Crawford, Ranking Member Himes, and distinguished Members of the Committee:

Thank you for the privilege of testifying before the House Permanent Select Committee on Intelligence. It is encouraging to see the Committee invest in a bipartisan examination of emerging challenges to national security and prosperity.

This hearing is occurring at a critical time because our nation and our intelligence community are struggling to adapt to four evolving threats to American security, prosperity and influence in the world:

- an axis of hostile aggressor states
- disruptive technologies
- the People's Republic of China's (PRC) economic aggression
- political subversion and cognitive warfare.

Axis of Aggressors

President Donald Trump's December 2017 National Security Strategy of the United States of America focused on the "growing political, economic, and military competitions" associated primarily with China and Russia's efforts to "erode American security and prosperity." Eight years later, that threat has become more dangerous as those two revisionist powers have expanded an axis of aggressors to include other authoritarian regimes hostile to the United States such as the Islamic Republic of Iran, North Korea, Cuba, and, until recently, Venezuela. Each member of the Axis pursues its own objectives, but they share a common

agenda to tear down the existing rules of international discourse and replace them with a new set of rules sympathetic to their authoritarian forms of governance and, in China's case, its statist, predatory economic model. They provide material, economic, financial, informational and diplomatic support to one another and apply each state's competitive advantages in concert to undermine U.S. security, prosperity, and influence.

The intelligence community is aware of expanding threats from the axis. The intelligence community must organize to identify and counter those threats, exploit vulnerabilities, and isolate the axis from sources of mutual support. Three opportunities to do so include:

- Build allied intelligence architecture to expose and operate against the axis through coordinated and sustained actions.
- Field predictive AI-enabled warning capabilities built on commercial and integrated data (e.g. imagery, RF, shipping, finance, insurance, logistics) to forecast coordinated behavior, and institutionalize commercially derived predictive intelligence as a standing mission capability rather than an ad hoc pilot or demonstration effort.
- Track flows across the axis of money, energy, weapons, and other sources of support to expose opportunities to interdict or disrupt those flows.

Understanding how the axis of aggressors employ and plan to employ disruptive technologies to undermine and threaten U.S. security is essential to developing

countermeasures, defending the homeland, and ensuring the effectiveness of U.S. military forces.

Disruptive Technologies

The axis of aggressors is increasing cooperation in the development and application of new technologies to strengthen their grip on power, gain asymmetrical advantage over the U.S. joint force, and attack or hold at risk critical U.S. and allied infrastructure at home, abroad, undersea, and in space. The United States faces this competition across the full spectrum of disruptive technology, from the exquisite to the accessible, and must hold overmatch at both ends.

At the exquisite end sit quantum systems, hypersonic weapons, counterspace weapons, directed energy, advanced materials, advanced semiconductors and computing power, and the training of frontier artificial-intelligence models. These demand vast capital, rare inputs, and specialized expertise, and they remain concentrated among a handful of advanced states and major corporations. Their scarcity concentrates decisive military power in the hands of the competitors able to afford them. A breakthrough in quantum computing that breaks the encryption protecting American networks; a hypersonic weapon that defeats missile defenses; a counterspace weapon that blinds the satellites the joint force relies on for warning, navigation, and communications; a directed energy system that changes the economics of air and missile defense; or a new class of materials that transforms what the joint force can build could each neutralize advantages the United States has held for a generation. These

technologies reward sustained national commitment, but money alone does not produce breakthroughs. The United States can lead at this end of the spectrum through well-resourced research, private capital, free-market competition, and its power to attract the world's best talent, advantages no authoritarian competitor can order into being. The United States must not cede that edge.

At the accessible end sit the everyday use of AI models, autonomous systems, biotechnology, and offensive cyber tools. These technologies draw on commercial markets and demand far less capital and infrastructure, placing them within reach of lesser states, terrorist organizations, and criminal networks. The cheap attritable drones transforming the battlefield show how quickly such capability spreads and how far it reaches. Even as the United States retains technical overmatch, competitors erode that margin with cheaper variants that, while less sophisticated, prove effective enough to close the distance to U.S. capability at a far lower cost. The hostile authoritarian states steal what they cannot develop themselves and often pass capabilities to proxies who extend the reach while masking attribution.

The intelligence community must help leaders deny the axis the advantages it seeks at both ends of the technology spectrum. Identifying how adversaries could weaponize critical supply chains and uncover adversary efforts to infiltrate sensitive government, private sector, and academic research enterprises must be a priority counterintelligence task. Investments in technologies will not result in competitive advantage if technologies are unprotected. Three opportunities for the intelligence community to safeguard technologies include:

- Identify the most critical technologies and intelligence prospects, establish security standards, and mobilize public and private efforts to protect them from espionage. Investors and companies should establish cybersecurity, physical security, and insider threat protection necessary to protect their investment.
- Identify gaps in research funding and talent in areas that risk ceding competitive advantage to adversaries so that the government and the private sector can use that information and analysis to prioritize investment in research and talent recruitment and development.
- Provide early warning of critical adversary technology and help leaders shift priorities to pursue the development of countermeasures.

Chinese Economic Aggression

The Chinese Communist Party has weaponized economic interdependence, using market access as coercion, engaging in systematic intellectual property theft, and deploying strategic investments to capture critical supply chains and emerging technologies. China's aggression goes far beyond traditional economic statecraft and is asymmetric in nature making it a direct threat to American prosperity, the American industrial base, and any technological edge the United States and allies possess.

Congress has attempted to respond to this threat through bills such as H.R. 5580 and S.295, neither of which have become law. The intelligence community has made progress in tracking Chinese intellectual property theft, but efforts remain fragmented and disconnected

from the vast amount of open-source data. The following are three opportunities for the intelligence community to help policymakers and legislators counter Chinese economic aggression:

- Elevate economic threats as a national security priority with a focus on supply chain vulnerability, critical technology competition, and strategic investment patterns.
- Institutionalize analysis of open-source intelligence like corporate filings, shipping data, academic partnerships, and patent applications to identify patterns of economic aggression such as industrial espionage, transshipment to evade trade enforcement mechanisms, and forced labor. The intelligence community should use private sector capabilities when possible.
- Develop private sector partnerships where declassified information can be shared with relevant stakeholders, particularly technology firms directly targeted by Chinese economic aggression. The intelligence community should simultaneously be learning from their private sector partners about Chinese tactics and emerging vulnerabilities.

Adapting U.S. intelligence institutions to understand and counter the Chinese economic threat is necessary for American security and prosperity.

Political Subversion and Cognitive Warfare

Political subversion and cognitive warfare[1] are not new threats to national security, but artificial intelligence capabilities such as the ability to generate convincing false text, video, and synthetic personas in seconds have accelerated and extended the reach of malign actors in the informational and cognitive domains. Moreover, the algorithms that drive content on social media platforms such as TikTok affect cognitive processes that transform information into beliefs, decisions, and behavior. The cognitive domain is vital to national security because without a shared sense of reality, credible information, and public trust, our nation may be unable to generate the popular will to confront aggression. Russia, China, and Iran are each engaged in sustained campaigns of cognitive warfare. Objectives include shifting the blame for their own acts of aggression, eroding Americans' common identity, and diminishing citizens' confidence in democratic principles, institutions and processes. Hostile authoritarian regimes combine censorship and surveillance at home with disinformation, misinformation, and propaganda abroad to prevent opposition to their regimes while sowing division and discontent in the United States and other free and open societies. Intelligence is essential to countering political subversion and cognitive warfare without compromising free speech.

The intelligence community is engaged in protecting U.S. citizens from cognitive warfare. The Federal Bureau of Investigation investigates foreign influence activities. The Cybersecurity and Infrastructure Security Agency (CISA) helps ensure citizens' confidence in

[1] "a form of warfare that focuses on influencing the opponent's reasoning, decisions, and ultimately, actions to secure strategic objectives without fighting or with less military effort" (ISW 2025)

elections. The Department of State tracks foreign propaganda and influence campaigns abroad. But no organization combines intelligence efforts to reveal the scope and assess the effect of political subversion and cognitive warfare. Moreover, there is no clear bridge from intelligence into policy development and operations to defend against the threat and conduct offensive operations in the informational and cognitive domains to undermine and impose costs on adversaries. Countering political subversion and cognitive warfare demands an evolution of intelligence organizations and capabilities in three areas:

- Form an interagency task force that includes private sector partners with the mission of exposing political subversion and cognitive warfare. Publish findings to educate the public and share information and intelligence with federal, state and local governments to take appropriate action. Emphasize exposing how hostile states operate through investment and acquisition, front organizations, targeted cultivation of officials and institutions, research and academic partnerships, and control of the platforms and infrastructure through which information moves. Provide policymakers, prosecutors, and citizens with an accurate attribution and expose adversary campaigns as they form rather than attempt to police content.
- Apply the intelligence-related lessons from other states that have been subjected to sustained campaigns of political subversion and cognitive warfare such as Ukraine, Finland, Estonia, Romania, Australia, and Taiwan.
- Identify opportunities to reach populations within authoritarian regimes with alternative sources of information to clarify U.S. intentions, counter

authoritarian regime propaganda, and undermine socio-cognitive methods of authoritarian state control.

Conclusion

While the emphasis in this statement has been on hostile nation states, it is important to recognize as we approach the twenty-fifth anniversary of the mass murder attacks of September 11, 2001, that our nation cannot neglect the threat from terrorist organizations and transnational criminal organizations. Those organizations become more powerful when they receive support from nation states (such as Pakistan's support for the Taliban, Haqqani Network, and Lashkar-e-Taiba; Qatar's support for Hamas; Maduro's support for various drug cartels; and Iran's support of Hamas, Hezbollah, the Houthis, and Hash de Shabi militias in Iraq). Moreover, the transfer of disruptive technologies to terrorist organizations such as advanced cyber tools, and artificial intelligence combined with bioengineering is 'democratizing destruction'. It will be important to remember the principal lesson of 9-11 that threats to the homeland that develop abroad can only be dealt with at an exorbitant cost once they reach our shores. The intelligence community must provide early warning of emerging non-state threats and support leaders in adapting the successful model of helping partners abroad fight terrorist organizations that threaten vital U.S. interests.