Wicked Problems Lab
Special Report

Dominating the Digital Space

A Whole-of-Society Strategy for Securing the United States from Cyber Aggression

Lt. Gen. (Ret) Charlie "Tuna" Moore
Distinguished Visiting Professor, Vanderbilt University

Brett Goldstein
Special Advisor to the Chancellor; Research Professor in Engineering Science and Management, Vanderbilt University

VANDERBILT UNIVERSITY
INSTITUTE OF
NATIONAL SECURITY
EDUCATE • INNOVATE • CONVENE • ADVISE

This Special Report was produced by the Vanderbilt University Institute of National Security's Wicked Problems Lab.

Front image: Cam/Adobe Stock.

About the Vanderbilt University Institute of National Security

The Vanderbilt Institute of National Security brings together leaders from government, academia, and industry to address the complex challenges shaping U.S. and global security. Through research, education, and public engagement, the Institute prepares the next generation of national security professionals to lead with character, insight, and purpose.

About the Wicked Problems Lab

The Wicked Problems Lab is an initiative in the Innovate pillar of the Vanderbilt Institute of National Security. The Lab brings cutting-edge research together with real-world expertise to develop pragmatic solutions to tackle national security challenges—bridging the gap between policy and implementation.

EXECUTIVE SUMMARY

The United States is engaged in an ongoing digital confrontation that threatens its economic and military strength, geopolitical leadership, and national security. Adversaries—most notably China—are exploiting cyberspace below the level of armed conflict by conducting persistent campaigns of espionage, intellectual property theft, data manipulation, and pre-positioning within critical infrastructure. These actions erode U.S. advantages and create the conditions to disrupt military mobilization and impose domestic hardship in a future crisis.

This Special Report argues that meeting these challenges requires a whole-of-society mobilization to achieve Digital Dominance, anchored by Analytic Superiority—the ability to sense, understand, and act at machine speed while degrading adversary decision systems. It proposes a focused approach to Integrated Resilience that prioritizes the five most essential critical infrastructure sectors and mandates real-time visibility, replacing voluntary and reactive information-sharing models with proactive federal insight and partnerships. This challenge will also require strengthened cooperation with trusted allies, whose shared intelligence, joint capabilities, and interoperable defenses are essential to countering globally distributed cyber threats.

Defensively and offensively, the United States must shift from episodic cyber actions to persistent cyber campaigning, updating operational authorities and scaling capacity through a National Cyber Operations Team (NCOT) that integrates private-sector expertise under direct military oversight, command, and control. NCOT can also support improved Title 32 efforts to protect critical infrastructure.

Finally, the Report emphasizes full integration of artificial intelligence into cyber operations to ensure speed, adaptability, and the capacity to respond effectively to emerging and unforeseen challenges. Collectively, these measures build the structural agility required to defend against digital aggression and secure U.S. leadership in the 21st-century global order.

THE CHALLENGE

The United States is engaged in a continuous confrontation, largely invisible to most of the American public, that carries profound national consequences. Malicious cyber activity affects every American institution, from households to hospitals to the nation's most important industrial sectors. Unlike past eras, the battlespace is no longer distant. It is embedded inside the nation's digital ecosystem—pervasive, persistent, and inseparable from daily life.

To meet this challenge, the United States must adopt a whole-of-society approach to cybersecurity, akin in strategic scope to the national mobilization required to win World War II, in close partnership with trusted friends and allies. The adversaries and methods are different, but the stakes—national security, economic prosperity, and geopolitical leadership—are the same.

THE STRATEGY

A successful mobilization requires a national North Star: Digital Dominance. Digital Dominance is not simply having the best hardware, software, or networks. It applies across the entire digital ecosystem—from sensors and transport infrastructure to analytic algorithms, AI-enabled decision tools, and the cyber-physical systems that can act faster than any adversary. Achieving Digital Dominance will generate lasting economic and military advantage, ensuring the United States shapes and controls the foundational technologies of the 21st century while preventing adversaries from undermining American security.

Within this broader national objective, the Department of War must pursue Analytic Superiority—the ability to leverage big data and AI faster and more effectively than our adversaries. Analytic Superiority is not only the ability to sense, understand, predict, and act faster than an adversary; it also requires denying adversaries the ability to do the same against us. It is a dual-action construct. While the U.S. fuses real-time data, AI-enabled analysis, and machine-speed operational decision-making to outpace opponents, it must simultaneously disrupt, degrade, manipulate, and confuse adversary sensing, analytic pipelines, AI models, and decision systems that are deployed to attack our interests. Analytic Superiority means ensuring the United States can see, think, and act clearly while adversaries operate in a state of persistent friction, uncertainty, and operational paralysis.

Achieving Analytic Superiority is not simply a technological challenge—it requires an institutional mindset that recognizes the digital environment, often referred to as the cyber domain, as central to modern warfare. Analytic Superiority is fundamentally about mastering this digital battlespace, and it is now a prerequisite for achieving air, land, sea, space, and information superiority. To meet this reality, the Department of War must cultivate a Department-wide digital culture in which cyber expertise is embedded into every warfighting domain and every warrior, while still preserving the elite cadre of high-end cyber operators required for the most complex missions. Foundational digital literacy must become universal across the force, even as specialized cyber warriors continue to execute advanced operations. Failing to do so risks isolating digital expertise from the operational contexts where it is most essential.

BEYOND DETERRENCE

A major distraction to achieving Digital Dominance and Analytic Superiority is the lingering hope of finally achieving cyber deterrence. Currently, there is no evidence that the U.S. can deter malicious cyber activity that occurs below the threshold of armed conflict/use of force; or, that cyber capabilities alone can deter other forms of aggression.

Most major destructive attacks—whether physical or digital—that rise to the level of armed conflict are already deterred by America’s nuclear and conventional capabilities. However, the overwhelming majority of adversary cyber operations—espionage, intellectual property theft, reconnaissance, data manipulation, and pre-positioning for future conflict—occur below the level of force. These operations are inexpensive, deniable, low-risk, continuous, and cause an erosion of our strategic standing.

China’s decades-long and undeterred intellectual property theft alone has cost us fortunes and likely saved Beijing trillions of dollars in research and development, fed the growing advantage of their manufacturing capabilities, and accelerated their national rise. Understanding this reality is essential to developing an effective national cyber strategy. Additionally, the lack of deterrence below the level of armed conflict/use of force sets the conditions for a far more serious challenge: the covert pre-positioning of foreign access within U.S. critical infrastructure and key resources (CIKR).

Adversaries—most notably China's "Volt/Salt Typhoon" actors—have already penetrated U.S. infrastructure networks. These intrusions are not attacks; they are deliberate steps to set conditions so that U.S. military forces cannot be rapidly transported into a war zone and to shape the strategic environment inside the United States itself. By positioning themselves within CIKR, China gains the ability to impose significant hardship on the American population at a time of its choosing. There is no legitimate espionage rationale for maintaining persistent access in the operational networks of the nation's most vital infrastructure unless an adversary intends, at some point, to generate disruptive effects that could sow fear, confusion, economic instability, political pressure, and a broader sense of national vulnerability—ultimately weakening public support for military operations and eroding national resolve in a crisis. The United States must clearly articulate a declared policy that pre-positioning in these systems will be treated as the digital equivalent of secretly emplacing explosives in critical infrastructure. And if such access is discovered in the future, all instruments of national power will be considered for an appropriate response.

This declaratory policy should not stand alone. It would be stronger if U.S. allies—especially NATO members and Indo-Pacific partners—adopt a similar declaratory policy. Shared acceptance of this principle would allow democratic nations to rapidly share intelligence, present a unified front and respond quickly, decisively, and collectively when such pre-positioning is uncovered, rather than treating these intrusions as some form of a "new normal." It would also begin to build collective will among like-minded nations to act beforehand, offensively and defensively, to ensure adversaries never succeed in these efforts.

A companion to this declaratory policy is a new operational concept: Integrated Resilience (IR). IR transforms fragmented cybersecurity efforts into a unified national posture capable of resisting, absorbing, and recovering from digital threats at scale. In order to operationalize IR, we need to focus on critical infrastructure. The U.S. currently designates sixteen sectors as critical infrastructure, a framework so broad that it obscures true priorities. When everything is critical, nothing is truly critical. A functional defense posture requires focusing national resources on the five sectors whose disruption would rapidly destabilize the country: power, water, telecommunications, finance, and healthcare/emergency services. These five sectors form the backbone of national resilience, and they depend on one another so completely that the failure of one can cascade into all the others.

For these five sectors, the U.S. must move beyond voluntary information sharing. The government cannot help defend what it cannot see. Even voluntary information—if done promptly—is a reactive approach to our security that cedes initiative to adversaries. Congress should enact legislation requiring key operators in the five critical sectors to provide real-time cyber telemetry and incident information to designated federal agencies, with strong protections mandating anonymization, removal of personal information, and safeguards for intellectual property. Existing frameworks such as CISA 2015 (the Cybersecurity Information Sharing Act, which enables voluntary threat-sharing between the private sector and government) and CIRCIA (the Cyber Incident Reporting for Critical Infrastructure Act, which requires companies to report major cyber incidents within set timelines) provide useful foundations, but they rely on voluntary or incident-based reports and are not designed for persistent, real-time visibility. Congress should also explicitly authorize the National Security Agency and U.S. Cyber Command to receive (from DHS) and analyze appropriately sanitized data for national security purposes, subject to stringent oversight and minimization.

"The government cannot help defend what it cannot see."

For the Department of War, the first priority within this construct must be Defense Critical Infrastructure (DCI). DCI is the subset of these essential sectors that directly enables U.S. military operations—bases, logistics hubs, transportation networks, energy providers, communications nodes, industrial facilities, and the civilian infrastructure required for mobilization and sustainment. Protecting DCI is not simply about national resilience; it is about mission assurance. The Department cannot project power, deploy forces, or sustain operations if the infrastructure it depends on is compromised or significantly degraded. DCI must therefore be the initial focus of DoW planning, visibility, analysis, and partnership efforts within the broader Integrated Resilience framework.

The Executive Branch must reinforce these measures with clear policy. The President should issue an Executive Order establishing Integrated Resilience, designating the five priority sectors, and creating a unified framework for real-time federal visibility and coordinated response options with state/local authorities. The National Security Council should update national cyber policy to reflect the new declaratory stance that unauthorized adversary access to these sectors is tantamount to preparing a destructive attack.

THE BEST DEFENSE

Even as the U.S. strengthens its defenses, offensive cyber operations must be recognized as one of our most powerful tools. Removing adversaries from our networks and foiling their plans requires sustained offensive pressure, not merely better defenses and reactive cleanup. The United States conducts highly capable but largely isolated “one-off” offensive cyber missions outside American networks, but these are discrete actions that achieve limited outcomes and lack the strategic coherence of a broader campaign. Our adversaries, by contrast, execute persistent cyber campaigns: continuous sequences of operations, tied together by shared goals, designed to shape the battlespace over time.

The nation cannot rely on episodic, manually approved operations if adversaries are operating continuously. The United States must shift to persistent cyber campaigning, whereby offensive cyber operations are conducted in a coordinated, ongoing sequence that disrupts adversaries’ planning cycles, imposes friction, degrades their capabilities, and keeps them on the defensive while posturing our forces for the potential of war. Persistent campaigning forces adversaries to devote resources to defense instead of offense, and limits their ability to prepare operations against the United States or its allies.

Implementing such an approach will require modest but important adjustments to the current U.S. cyber policy framework. Authorities governing offensive cyber operations—particularly NSPM-13/21—should be updated to endorse continuous campaigning, streamline operational approvals for certain classes of foreign-targeted cyber actions, and expand standing authorities for U.S. Cyber Command.

To scale offensive campaigning capacity, the United States must also build a far more ambitious construct: a National Cyber Operations Team (NCOT) that unifies government and private-sector cyber talent into a single, integrated team-of-teams under the operational control of U.S. Cyber Command.

Regardless of what internal organizational constructs the Department may consider, no combination of authorities, structures, or Service reforms will allow the DoW to scale to the level the nation now requires. The demand signal is too large, the threat landscape too dynamic, and the technical talent pool too competitive for the Department to meet future requirements with government personnel alone. One viable pathway to achieving the necessary scale and operational tempo is through the creation of NCOT, which integrates private-sector expertise with military command authority. NCOT will provide the nation the capacity, agility, and innovation needed to compete and prevail in the digital battlespace.

"No combination of authorities, structures, or Service reforms will allow DoW to scale to the level the nation now requires."

The Executive Branch should direct the Department of War and U.S. Cyber Command to stand up NCOT and explicitly authorize the Command to recruit, certify, and operationally employ private-sector teams in support of persistent cyber campaigns. These teams must operate under the Command's rigorous training, certification, and security standards, with clearly defined clearance pathways and rules of engagement. NCOT elements should be fully integrated into joint planning, targeting, and operational frameworks to ensure unity of command and seamless employment alongside Title 10/50 forces.

To ensure rapid completion and avoid the bureaucratic inertia that has historically slowed or derailed initiatives of this nature, the Commander of U.S. Cyber Command should be charged with developing and executing a detailed blueprint that defines the tasks, timelines, and dependencies required to operationalize NCOT as rapidly as possible, including any enabling support required from other departments and agencies. The President should approve the blueprint and receive regular progress updates from the Secretary of War and the Director of National Intelligence until NCOT achieves full operational capability. Congress should reinforce this presidential action by formally recognizing NCOT as a national cyber capability, establishing dedicated funding streams, and providing liability protections necessary for sustained private-sector participation.

The NCOT force will operate exclusively under the persistent oversight and command and control of U.S. Cyber Command's Title 10 forces. Success in the cyber domain requires strict adherence to one of the fundamental principles of war: unity of command. Without a single, accountable operational authority, cyber operations risk devolving into fragmentation, conflicting actions, and unintended effects that could generate strategic escalation. Additionally, while NCOT civilians can develop, prepare, and posture offensive capabilities up to the point of execution, current law and policy prohibit them from taking the final operational action that generates a cyber effect. Accordingly, civilian teams can carry the mission forward to the 'last tactical mile,' with execution handed off either to a uniformed operator physically embedded with the team, handed off in the virtual environment to a uniformed member at the moment of action, or—should Congress and the Department of War choose to update statutory authorities—empower NCOT civilian operators to execute effects in the future. NCOT is designed to scale national cyber capability, not to decentralize it. By placing all NCOT elements under Cyber Command's unified command structure, the United States ensures that expanded capacity strengthens coherence, discipline, and strategic alignment rather than introducing chaos into an already volatile operational environment.

It should also be noted that although NCOT is anchored in Title 10 command and control, its underlying operational framework could also be leveraged to help operationalize the visibility and information-sharing requirements outlined earlier for defending critical infrastructure—particularly by scaling the effectiveness of Title 32 National Guard cyber forces operating in support of state and national resilience.

While pursuing the establishment of NCOT, the Department of War must continue to fully empower U.S. Cyber Command to execute its critical missions while ensuring that the Command and the Services—working together—sustain the remarkable progress they have already achieved in recruiting, training, and developing the military's cyber workforce. This partnership has produced the highest-performing and highest numbers of cyber operators the nation has ever fielded, and it must be strengthened, not disrupted. Cyber Command must continue to receive full support in exercising its new authorities to establish training and certification standards across the Department's Cyber Operations Forces, ensuring a cohesive, interoperable, and mission-ready cadre. The Command must likewise be supported in executing its expanded acquisition authorities, which allow it to manage and execute its own budget, field capabilities at operational speed, and adapt more rapidly to emerging threats. These "service-like" authorities are essential to developing and maintaining the core corps of cyber warriors upon which the Joint Force, to include the NCOT, will depend.

EMBRACE AI, POSTURE FOR AN UNCERTAIN FUTURE

"Cyber conflict is increasingly fought at machine speed."

Finally, none of these actions will succeed without fully integrating artificial intelligence into all aspects of cyber operations. Cyber conflict is increasingly fought at machine speed. Without AI, human operators cannot detect, analyze, or respond fast enough to match adversaries who rely heavily on automation and AI-enabled reconnaissance and operations. Congress should authorize major investments in AI-enabled cyber defense and AI-driven offensive capabilities, including test ranges, evaluation centers, and mission-specific research programs. The Executive Branch should issue an Executive Order directing all relevant federal departments to integrate AI into cyber defense and mission planning, and establish clear guidance for when certain cyber offensive and defensive operations may be autonomously executed.

Even as the United States focuses on the threats and technologies we can anticipate today, we must remember that many of the most consequential developments of the digital age proved unpredictable. Only a few years ago, most people had never heard of a large language model; today, they are reshaping the digital landscape and transforming cyber operations. In the coming decade, we may face breakthroughs in quantum computing, synthetic intelligence, autonomous code generation, or entirely new paradigms of networking, sensing, or attack.

We know that some technologies—such as post-quantum cryptography—are inevitable and must be planned for now. But many others will emerge rapidly and unexpectedly. The nation needs not just strong defenses and powerful offensive capabilities, but a structural foundation that provides speed, agility, and adaptability in the face of future uncertainty.

The steps recommended in this paper—Integrated Resilience for the five most essential sectors, mandatory visibility into threats, persistent cyber campaigning, the creation of a unified National Cyber Operations Team, and the full integration of AI—provide exactly that foundation. They do more than prepare the United States for the threats we can already foresee. They create the institutional muscle memory, the operational agility, and the decision-making speed necessary to respond effectively to technologies and threats that have not yet emerged. They do so, moreover, while complementing and protecting the American technology sector that has become the envy of the world, not to mention the civil liberties and privacy protections that we expect and treasure.

By building a system that can see threats early, anticipate and confront proactively, respond quickly, campaign continuously, and integrate new tools rapidly, the United States positions itself not only to win today's digital battles but to thrive amid the unpredictable challenges of tomorrow.

CONCLUSION

The United States is in the midst of a global and protracted digital conflict. Adversaries exploit cyberspace to accumulate strategic advantage while remaining below international legal understanding of the use of force. Without swift and sustained action, the nation risks long-term strategic decline—or a devastating military defeat. A whole-of-society approach—anchored by Digital Dominance, Analytic Superiority, Integrated Resilience, a clear declaratory policy regarding adversary pre-positioning, a protected visibility framework for the five essential CIKR sectors, persistent cyber campaigning, a unified National Cyber Operations Team, and deep AI integration—is essential. These measures are not merely improvements; they are the highest-priority actions the nation must take to preserve its security and leadership in the digital age. The nation that achieves Digital Dominance will shape the global order for decades to come. The United States must ensure it is that nation.

ACKNOWLEDGEMENTS

The Institute of National Security acknowledges the support of the Vanderbilt University Office of the Provost through the Discovery Vanderbilt initiative as well as the Office of the Chancellor, the School of Engineering, College of Arts & Science, and Peabody School of Education for their collaboration and assistance. The Institute also thanks our generous donors for investing in the professional development of the next generation of U.S. national security professionals.