Cybersecurity: Deterrence Policy

January 18, 2022

Congressional Research Service
https://crsreports.congress.gov
R47011

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47011

January 18, 2022

Chris Jaikaran
Analyst in Cybersecurity Policy

Cybersecurity: Deterrence Policy

Many policymakers have embraced *deterrence* as a driving policy position for addressing attacks in cyberspace. However, deterring attacks remains elusive as nations disagree on acceptable behavior and criminal groups proliferate. This CRS report examines the policy of deterrence, how it may be implemented, and options for Congress.

Deterrence policy relies on established rule of behavior, the ability to detect violations of those rules, and capabilities to reliably employ against perpetrators. Efforts have been made to address some of these policies, such as with establishing norms and improving attribution; however, work remains for others.

Generally, cyberspace deterrence strategies seek to influence an adversary's behavior, discouraging them from engaging in unwanted activities. In contrast, denial strategies endeavor to improve a technology, process, or practice so that despite adversarial ventures, a cyberattack might have a low rate of success. Congress and the President have a history and practice in examining and implementing denial strategies, which may account for why many of these policy proposals have seen progress. Conversely, deterrence strategies have been implemented at a lower rate, despite broad recommendations for their use.

Cyberspace presents challenges for established deterrence strategy. Traditionally, deterrence relies on a few, known actors having the resources to develop and maintain a capability (as well as the intent to use it), and a history of known consequences being applied if norms are violated. Arguably, the inverse of these conditions exists in cyberspace. It is relatively cheap for malicious actors to acquire the knowledge and tools necessary to conduct cyberattacks so there are many potential adversaries, and there is ambiguity around retaliatory consequences for cyberattacks.

The Cyberspace Solarium Commission promoted a "layered cyber deterrence" strategic approach to addressing threats in cyberspace. The concept was introduced in their final report and reiterated across subsequent white papers, where 109 recommendations for Congress and the President were made. As the second anniversary of the Commission's final report nears, their recommendations can be tracked by their implementation status and analyzed by how those recommendations affect the strategic environment. Using taxonomies developed by the Department of Defense, the few recommendations that would have a deterrence effect have not been implemented. Most of the Commission's recommendations would deny an adversary's ability to conduct cyberattacks, and this may arguably create a secondary deterring effect. The deterrence recommendations include working on norms, establishing responses to attacks, and improving government organization.

With regard to norms, two United Nations working groups have agreed to 11 norms of responsible state behaviors in cyberspace. However, these norms are nascent and it remains to be seen how nations will adhere to and follow the norms. The United States could lead in this space by directing agencies to actively participate in norms maturation and engage international standards-setting bodies on information and communication technologies.

To bolster response capabilities to attacks, some have proposed declaring predictable response options. The European Union developed a "Cyber Diplomacy Toolbox" describing the actions perpetrators may expect if they conduct cyberattacks against member states. The United States has not publicly disclosed a menu of response options, but has used some in the past, such as public attribution and sanctions. Policymakers may choose to direct the development of such an options list. But to be effective as a deterrent, it would need to be consistently followed.

Lastly, to better structure federal governance of cyber deterrence, Congress and the executive branch have pursued the creation of a bureau within the Department of State responsible for cyberspace diplomacy. Such a bureau could lead efforts related to norms setting, foreign assistance, and confidence-building measures. However, outstanding questions for policymakers exist, including how the bureau would coordinate with other federal agencies—many of which have significant technical capabilities and already engage in international fora—and to what extent the bureau would be responsible for representing the United States in multilateral and civil society fora addressing cybersecurity issues.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

The United States government has long sought to effectively deter (or stop) cyberattacks and to respond to attacks in a manner that prevents future ones. Both goals have appeared elusive as the frequency of cyberattacks, from petty to significant, have increased over time.[1] These attacks show that deterrence is difficult to achieve in cyberspace. There are nuances surrounding cyberattacks that invert previous notions of deterrence policy. Despite challenges, many regard deterrence as a necessary step to establishing order for cyberspace operations, and as a building block for future actions, and policymakers continue to pursue a strategy of deterrence for cyberspace and cyberattack. This report analyzes the strategy of deterrence in relation to cyberattacks and discusses options Congress may pursue in advancing deterrence policy.

In March 2020 the Cyberspace Solarium Commission (Commission) launched its report advocating for a "layered cyber deterrence" strategic approach for cybersecurity.[2] As the second anniversary of the Commission's report approaches, policymakers may seek to examine a deterrence strategy in light of recent advancements in cybersecurity policy and recently evolved cyberattacks.

While this report discusses deterrence policy strategically, it does not discuss in depth potential capabilities related to deterring cyberattack. Policies surrounding the use of instruments of national power (e.g., diplomacy, intelligence activities, armed forces, and sanctions) are not significantly discussed in this report.[3] Types of attacks also are not discussed in this report, as deterrence policy is intended to apply broadly to all types of attacks.[4]

The Cyberspace Solarium Commission

The John. S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY2019 NDAA, P.L. 115-232) established the Cyberspace Solarium Commission (Section 1652) to develop approaches to defend the United States against significant cyberattacks. The FY2019 NDAA expressly directed the Commission to examine policies around norms, denial, and deterrence. The statute directed the Commission:

> To review and make determinations on the difficult choices present within such options, among them what norms-based regimes the United States should seek to establish, how the United States should enforce such norms, how much damage the United States should be willing to incur in a deterrence or persistent denial strategy, what attacks warrant response in a deterrence or persistent denial strategy, and how the United States can best execute these strategies.

In its final report, the Commission advocated for a strategic approach of **layered cyber deterrence** and promoted three ways to achieve this end state.

---

[1] Embroker, "2021 Must-Know Cyber Attack Statistics and Trends," webpage, December 10, 2021, at https://www.embroker.com/blog/cyber-attack-statistics/.

[2] Cyberspace Solarium Commission, final report, March 2020, at https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Also, see CRS In Focus IF11469, *The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence*, by Chris Jaikaran.

[3] A discussion of the use of military force in cyberspace may be found in CRS In Focus IF11995, *Use of Force in Cyberspace*, by Catherine A. Theohary.

[4] Cyberattacks and a discussion of them may be found in CRS Report R46974, *Cybersecurity: Selected Cyberattacks, 2012-2021*, by Chris Jaikaran.

- **Shape Behavior**—working with partners to influence how parties act in cyberspace.
- **Deny Benefits**—securing critical networks (e.g., infrastructures and governments) and working to create systemic security and resiliency in cyberspace.
- **Impose Costs**—retaliating against malicious actors who use cyberspace to harm the United States.

The Commission viewed "deterrence [as] an enduring American strategy."[5] In the Commission's view, deterrence is about imposing costs on adversaries. Within the confines of the report, the Commission saw deterrence incorporating two concepts. First, the Commission acknowledges that many of their recommendations are designed to achieve deterrence through denial—that is, improving defense so to make it more expensive for adversaries to carry out attacks. Second, the strategy promotes defending forward—that is, continually detecting, hunting, and opposing adverse behavior in cyberspace to increase their costs of operating.

Since the report's release, the Commission has published additional white papers, legislative proposals, and a progress report. The Commission recommended 109 actions in those documents that Congress and the President could take to implement this strategic approach. A list of the recommendations and their status can be found in the **Appendix**. Using descriptions of denial and deterrence (found in "Deterrence Factors" section) the recommendations are analyzed and arranged according to their ability to enable strategies of denial, deterrence, or both. **Table 1** provides a count of the recommendations by their implementation status (i.e., some action taken by the President or Congress) and strategy categorization.

Table 1. Count of Cyberspace Solarium Commission Recommendations

By Recommendation Status and Strategy Categorization

Recommendation Status	Deny	Deter	Both
Implemented	11	0	10
Nearing Implementation	10	1	6
On Track	28	4	15
Delayed	8	2	0
Significant Barriers	3	0	1
TOTAL	**60**	**7**	**42**

Source: CRS analysis of Cyberspace Solarium Commission, "2021 Annual Report on Implementation," report, August 2021, at https://drive.google.com/file/d/19V7Yfc5fvEE6dGloU_7bidLRf5OvV2__/view.

Examining the distribution and status of recommendations, the lower number of deterrence-related recommendations and their comparative lack of implementation stands out. This may be because of the relative difficulty of implementing deterrence policy, which is discussed in the "Response Options" section of this report. It may also be because denial strategies are more direct and Congress has experience addressing those types of activities.

For instance, some denial activities that have been implemented through recently enacted legislation seek to strengthen the authorities of the Cybersecurity and Infrastructure Security

[5] Cyberspace Solarium Commission, "Report," webpage, February 12, 2021, at https://www.solarium.gov/report.

Agency (CISA)[6] and address a perceived gap in national cybersecurity resiliency by improving kindergarten to high school cybersecurity capabilities.[7] In addition, the Fiscal Year 2022 National Defense Authorization Act included provisions pertaining to vulnerability identification (Section 1544) and information sharing (Section 1548).[8] In these examples, Congress passed legislation implementing one or more of the Commission's recommendations, and in both sets of examples the recommendations affected domestic actors for which legislation or executive action is directly effective.

Some recommendations—such as those related to exercises—may enable both strategies. Exercises may promote denial (i.e., hindering or preventing an adversary from launching successful attacks) by building partner confidence in capabilities and use of those capabilities so that further coordinated actions are possible. Exercises may also promote deterrence (i.e., influencing adversaries' behaviors) by showing cyber operation capabilities in an effort to highlight that the capabilities will outmatch an opponent's.[9]

Deterrence Factors

While Congress and the President have pursued policies of deterrence in cyberspace, their actions to date have primarily focused on denying adversarial actions. At times, this focus is intentional; the Department of Defense's (DOD) strategy of "persistent engagement" seeks to occupy adversaries and deny them the time and resources to carry out attacks.[10] At times, it is consequential, such as pursuing strategies to impose costs on adversaries, thus denying gains of attacks or resources for future attacks. Because of this historical prominence of implementing denial strategies, it may be helpful to consider deterrence policy contrasted against denial policy for context and comparison.

Denial and deterrence cybersecurity strategies are different approaches to achieve the same goal: a safer digital environment. These strategies are not mutually exclusive. As seen by the Commission's recommendations, particular activities can serve both strategies, and combining activities can have a multiplier effect on the actions.

Generally, for cybersecurity, denial strategies seek to improve technology, processes, and practices over something in one's own control so that despite an adversary's efforts, their success rate is low. Deterrence strategies seek to affect the behavior of other individuals or entities—stopping them from engaging in an unwanted activity. The DOD developed descriptions of "denial" and "deterrence," which are used in this report in the context of cybersecurity to categorize activities and provide a framework for discussing policy options.

[6] P.L. 116-283, §1716.

[7] P.L. 117-47.

[8] P.L. 117-81.

[9] An example of an information sharing-related recommendation is 3.3.4 on expanding coordinated cyber exercises. For further information on the utility of cyber exercises, see National Security Archive, "BALTIC GHOST: Supporting NATO in Cyberspace," webpage, December 6, 2021, at https://nsarchive.gwu.edu/briefing-book/cyber-vault/2021-12-06/baltic-ghost-supporting-nato-cyberspace.

[10] Department of Defense, "Summary, Department of Defense Cyber Strategy," 2018, at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Glossary

Denial	A denial measure is an action to hinder or deny the enemy the use of territory, personnel, or facilities. It may include destruction, removal, contamination, or erection of obstructions.[11]
Deterrence	Deterrence prevents adversary action through the presentation of a credible threat of unacceptable counteraction and belief that the cost of the action outweighs the perceived benefits.[12]

The definition of denial can be interpreted as stopping the adversary from using something. For this interpretation, many potential cybersecurity activities satisfy the definition. For example, disrupting an adversary's internet infrastructure (e.g., a botnet[13]) inhibits their malicious use of cyberspace as a domain, and proper configuration and maintenance of one's own information and communications technology (ICT) denies an adversary the opportunity to exploit it. Unique to this interpretation is the focus not on the adversaries themselves, but instead on the things they seek to exploit (e.g., unpatched ICT).

The definition of deterrence can be interpreted as influencing the adversary in such a way as to prevent their engaging in malicious behavior. In this model, deterrence relies on norms and demonstrated capabilities. Nations will need to understand what other nations consider acceptable versus unacceptable (violating) behaviors, a government will need capabilities to influence the behavior of other governments as well as non-state actors, other nations will need to believe that the capabilities will be used, and the government's intentions will need to be messaged to potential adversaries. It is arguable that for cyberspace, these conditions are nascent or do not exist.

Conventional deterrence policy relies on a few conditions: there is a high cost to develop, maintain, and use certain offensive capabilities; there are a limited set of actors with those capabilities; if actors choose to use the capabilities, then they will incur known consequences; and there is a history of norms compliance upon which to rely.[14]

Cyberspace arguable is characterized by the inverse of those conditions: the cost of entry for potential malicious actors is low; there are many potential malicious actors to address (both state and non-state); the retaliatory consequences for successful cyberattacks are ambiguous or unknown; and there is not a long history of norms compliance.

It is for this reason that some suggest that deterrence in cyberspace is not a viable strategy.[15] The Commission recognized that Cold War-era analogies of deterrence are likely not applicable in cyberspace, yet considered that some form of deterrence may be achievable, especially through improved security measures and behavior shaping.[16]

---

[11] Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, October 22, 2018, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

[12] Joint Chiefs of Staff, *Barriers, Obstacles, and Mine Warfare for Joint Operations*, Joint Publication 3-15, Washington, DC, March 5, 2018, pp. II-7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_15.pdf.

[13] "The word '*botnet*' is formed from the words 'robot' and 'network.' Cyber criminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all the infected machines into a network of "bots" that the criminal can remotely manage." National Institute of Standards and Technology, "Botnet" glossary entry, at https://csrc.nist.gov/glossary/term/botnet.

[14] Director of National Intelligence, *Global Trends 2040: A More Contested World*, March 2021, at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[15] Michael Fischerkeller and Richard Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Foreign Policy Research Institute*, Summer 2017, pp. 381-393.

[16] "The Process of the U.S. Cyberspace Solarium Commission—CyCon 2021," NATO Cooperative Cyber Defence

For deterrence activities, it is important to consider non-cyberspace-based responses to cyberspace-based incidents. Cybersecurity experts can help identify and frame issues to consider when examining deterrence strategies, but the range of activities available to government agencies to influence adversaries is far greater than those within the cybersecurity field. Experts across fields will be necessary to provide multidisciplinary solutions for effective deterrence strategies. Experts to consider consulting when drafting deterrence actions include those for specific countries (e.g., Russia, China, North Korea and Iran)[17] and experts in the capabilities policymakers are seeking to employ (e.g., diplomatic, intelligence, military, or economic). This position is reinforced by cybersecurity experts who view cyberattacks as a challenge for the computer science community, but for which solutions cannot be purely technical.[18]

It has long been the policy of the United States government that responses to cyberattacks will be proportional, but may not be limited to cyberspace operations only.[19] Experts believe that the U.S. government has not fully embraced this posture, but doing so may be necessary to deter future cyberattacks.[20]

Limits Related to Cyber-Only Responses to Cyberattacks

Some Members of Congress have expressed frustration with the lack of public discourse surrounding cyberattacks and the U.S. government's response capabilities.[21] Such discussions are frequently held in classified venues, thereby excluding public scrutiny. While this practice may limit debate, offensive cyber response capabilities are a fragile resource, and publicizing them may reduce their effectiveness.

For a government, it takes research and operational security to discover, develop, and deploy offensive cyber capabilities in a manner that allows for repeated use and covert or clandestine action. This is especially true for attacks on systems that have regimented security procedures, such as those of a foreign government agency.

The moment an attack is discovered, access to the breached systems may start to disappear, evidence may be collected that attributes the attack to those behind it, and additional operations they have may become vulnerable, especially if they shared operational infrastructure or techniques, tactics or procedures. In the event that the United States were to have its capabilities disclosed as part of public discourse, it too may lose the ability to use those capabilities.

For the public debate on capabilities, it is also important to consider the difference between conventional weapons and offensive cyber capabilities. Conventional weapons are developed for

Center of Excellence, May 25-28, 2021, at https://www.youtube.com/watch?v=OBUy7aGNiCQ.

[17] For more information on attacks from these countries, see CRS Report R46974, *Cybersecurity: Selected Cyberattacks, 2012-2021*, by Chris Jaikaran.

[18] Dmitri Alperovitch, "The Case for Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions," *Foreign Affairs*, January/February 2022, at https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.

[19] Intelligence Matters Podcast, "National Cyber Director Chris Inglis on Deterring Cyber Threats," *CBS News*, November 24, 2021, at https://www.cbsnews.com/news/national-cyber-director-chris-inglis-cyber-threats-intelligence-matters-podcast/.

[20] Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs*, January/February 2022, at https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

[21] For an example, see U.S. Congress, House Committee on Oversight and Reform, *Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats*, 117th Cong., 1st sess., November 16, 2021.

use *in* a domain. Defending against those weapons may also use some other tool applied *in* that domain. For example, a ballistic missile may be intercepted by an anti-ballistic missile system in the air before it hits the intended target.[22] However, an offensive cyber capability usually exploits a weakness *against* the domain—or a weakness against a system or network itself in cyberspace. Thus, defending against a cyberattack may include the development and use of a new tool, or patching an existing system to mitigate the effect of an offensive cyber tool.

Norms

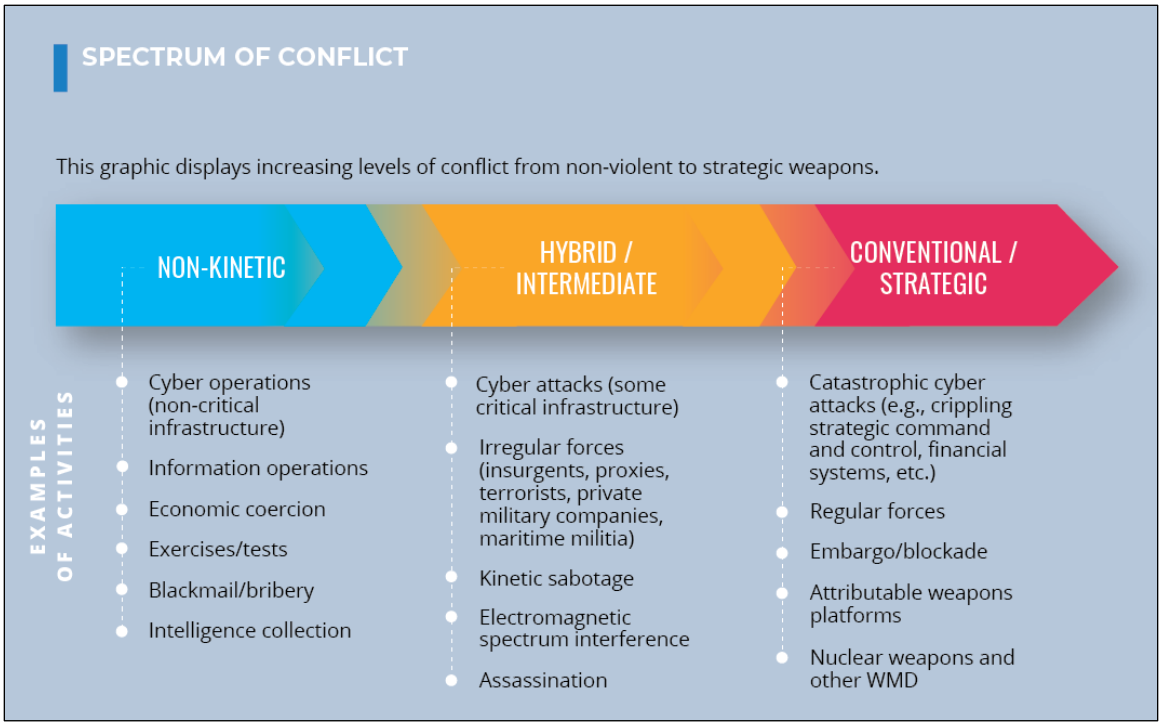
"Norms," some experts assert, "can be understood as rules for behaving that forbid or encourage certain activities."[23] A challenge to normative behavior in cyberspace is that cyberspace is a domain where behaviors occur, and cyberspace operations are tools of national power that nations may choose to employ. As Congress examines cyberattacks and responses to them, it may be helpful to consider the duality that cyberspace is both a domain and a capability. For example, cyberattacks can occur within cyberspace (e.g., data and identity theft attacks) and can occur against cyberspace itself (e.g., attacks against cloud service providers). In both types of attacks information and communications technology (ICT) is used and harmed, and it is that harm that nations may seek to curtail with norms.

The development of norms in the context of deterring cyberattacks is further complicated by the fact that cyber operations can occur across the entire spectrum of conflict ranging from localized, nonviolent incidents to far more consequential events with potentially national consequences. As shown in **Figure 1**, the Office of the Director of National Intelligence sees cyber operations as spanning the full range of such incidents.

[22] For information on ballistic missile defense, see CRS In Focus IF10541, *Defense Primer: Ballistic Missile Defense*, by Stephen M. McCall.

[23] Dr. Martin C. Libicki, "Norms and Normalization," *The Cyber Defense Review*, Summer 2020, at https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2004_Libicki_WEB.pdf.

Figure 1. Spectrum of Conflict



Source: Adapted from Director of National Intelligence, *Global Trends 2040: A More Contested World*, March 2021, at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

Notes: WMD=Weapons of Mass Destruction.

Aggressive nations may explore the use of limited cyberspace operations as an alternative to other types of attacks and opt to use cyberattacks as a tool to reduce other forms of conflict. Cyberspace operations may be adopted by adversarial nations if they believe that victim nations will adhere to a norm that responses to aggression be proportional. If aggressive nations pursue this strategy, it is likely that cyberattacks will increase in frequency as a tool in the lower spectrum of attacks.[24] This strategy would seek to force proportional (i.e., cyber) response from victim nations and seek to inhibit the use of other instruments of national power.

For example, it is not normative for military capabilities to be used in response to criminal activity. However, repeated cyberattacks have led policymakers to explore novel uses of capabilities as adversaries have escalated attacks and the impacts of those attacks have become more severe. One such case is the combatting of ransomware, which has the effect of degrading U.S. infrastructure in a way that may result in the endangerment of civilian populations (e.g., a ransomware attack against a hospital).[25] In response, decisionmakers have employed military capabilities to learn about ransomware gangs and move against them.[26]

[24] Director of National Intelligence, *Global Trends 2040: A More Contested World*, March 2021, at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[25] Ransomware-as-a-Service (Raas) operators are able to replicate and deploy potentially destructive attacks across a variety of potential victims, many times over, without regard for the business or services that the victims provide.

[26] Julian E. Barnes, "U.S. Military Has Acted Against Ransomware Group, General Acknowledges," *New York Times*, December 5, 2021, at https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.

Cyberattacks may increase because nations view cyberspace as a novel operational domain without established rules of engagement. In such a lax environment, opportunities to test techniques, tactics, and procedures are plentiful both for attacks and responses. The National Intelligence Council assessed the outlook for international norms.[27] That assessment placed norms on a spectrum:

- *Norms least likely to be contested* are those that are broadly accepted by nations and for which violations are widely condemned (e.g., national sovereignty).
- *Norms likely to experience regional variations* are those where their acceptance is not broad (e.g., environmental protections).
- *Norms at risk of weakening* are those for which a major national power has already breached it or for which implementation has been curtailed (e.g., open commerce).
- *Norms in early development* are those not fully agreed to, not widely accepted, or for which a future is unclear (e.g., cybersecurity).[28]

Concurrently, two United Nations working groups have developed a common set of norms for responsible state behavior in cyberspace. The first is the Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). It is the older and smaller of the two with 25 member nations. The second group is the Open-Ended Working Group (OEWG), which is newer and larger and includes any interested nation. Russia was an original sponsor of this group, despite the existence of the GGE. The United States was an original supporter of the GGE and participated in the OEWG discussions.

In 2015, the GGE published a note where the group agreed to 11 norms.[29] In 2021, the OEWG released their final substantive report reinforcing those same 11 norms.[30] These norms for responsible state behavior in cyberspace are

1. Nations agree to cooperate;
2. Nations will consider all source information when making claims of attribution;
3. Nations will not knowingly allow their territory to be used to conduct cyberattacks;
4. Nations will share information;
5. Nations will respect human rights and secure ICTs to do so;
6. Nations will not knowingly use ICT to damage critical infrastructure;
7. Nations will appropriately protect their own critical infrastructure;
8. Nations will respond to requests for assistance from other nations;
9. Nations will take steps to secure supply chains;

[27] Director of National Intelligence, *Global Trends 2040: A More Contested World*, March 2021, at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[28] Ibid.

[29] Note by the Secretary General, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015, at https://undocs.org/pdf?symbol=en/A/70/174.

[30] Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, "Final Substantive Report," A/AC.290/2021/CRP.2, March 10, 2021, at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

10. Nations will support the reporting of vulnerabilities; and
11. Nations will not attack computer emergency response teams.

Relative to other international norms—such as those related to national sovereignty and defense—cybersecurity norms are in early development and adoption. It remains to be seen how nations will operate within those norms.[31]

The U.S. government has already taken overt actions in support of some of these norms. For example, the U.S. Intelligence Community published a white paper on attributing cyberattacks that takes into consideration open-source information.[32] Federal agencies have launched efforts for supply chain security and vulnerability disclosure.[33] Congress has directed federal agencies to engage partner nations for cybersecurity and increase information sharing activities.[34]

The U.N.'s ICT security efforts have been following a dual path of security fields. The first field addresses demilitarization, de-escalation, and prevention as they relate to nation-state actors. That is the field under which these 11 norms were developed. The second field is on cybercrime and non-state actors. Russia proposed a U.N. resolution to establish an ad-hoc group to address cybercrime and state sovereignty, which was agreed to by the General Assembly.[35] Some observers believe this is an effort to replace the existing order on international cybercrime and internet freedoms.[36]

Regardless of a nation's intentions behind engaging in norms-setting activities, many nations agree that norms development is a worthy pursuit. While development is occurring, it is important to consider that these efforts are the beginning of a lengthy process. It takes time for norms to be developed and agreed to. It takes even more time for states to change their behavior and the norms to become common practice. Despite the far-off potential for return on investment, experts believe that norms are a vital pursuit, necessary for peaceful operations in cyberspace.[37]

Response Options

Certainly, having the ability to determine perpetrators is a key element to deterrence. If perpetrators believed that they would never be identified, then they would not have to fear retaliatory action. Historically, barriers to effective response have included the difficulty in adequately attributing cyberattacks, the time it takes to do so, and the availability of information for public discussion related to attribution. However, the U.S. government has recently released

[31] Director of National Intelligence, *Global Trends 2040: A More Contested World*, March 2021, at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[32] Office of the Director of National Intelligence, "A Guide to Cyber Attribution," memo, September 14, 2018, at https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

[33] Cybersecurity & Infrastructure Security Agency, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," website, at https://www.cisa.gov/ict-scrm-task-force. Cybersecurity & Infrastructure Security Agency, "Develop and Publish a Vulnerability Disclosure Policy," *Binding Operational Directive 20-01*, September 2, 2020, at https://cyber.dhs.gov/bod/20-01/.

[34] United States-Israel Advanced Research Partnership Act of 2016 (P.L. 114-304).

[35] United Nations, "General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations," press release, May 26, 2021, at https://www.un.org/press/en/2021/ga12328.doc.htm.

[36] Joyce Hakmeh and Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet," *Council on Foreign Relations Blog*, January 13, 2020, at https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

[37] Joseph S. Nye, Jr., "The End of Cyber-Anarchy? How to Build a New Digital Order," *Foreign Affairs*, January/February 2022, at https://www.foreignaffairs.com/articles/world/2021-12-14/end-cyber-anarchy.

information on a slew of cyberattacks, attributing them not just to nations or criminal organizations, but to individuals. The government has decreased the time it takes to make these attributions and has also made public the information agencies used to determine potentially guilty parties. A further discussion of attribution can be found in CRS Report R46974, *Cybersecurity: Selected Cyberattacks, 2012-2021*, by Chris Jaikaran. While work remains to improve confidence in attribution and decrease the time it takes to attribute attacks, it appears that attribution is no longer the barrier it used to be.

Having a level of attribution is a key step in responding to cyberattacks. But once a nation has confidence in potential perpetrators, the nation will need to decide if tools will be employed against those perpetrators, which tools against which perpetrators, and for how long.

Identifying a slate of options that nations intend to use in response to cyberattacks serves two potential purposes: (1) it signals to adversaries the actions victim nations are prepared to engage in to retaliate for attacks; and (2) it publicizes the options for its citizens so that they may debate with their elected leaders the appropriateness and suitability of those options. A long-standing criticism of cyberattack response in the United States is that the federal government has not revealed its menu of options. This is despite both congressional[38] and executive[39] direction to the U.S. Department of State to report on cyberspace policy.

The State Department has issued papers discussing elements of the policies but has generally not discussed specific retaliatory options publicly.[40] Some have argued that limiting public information about exact plans allows the United States to remain agile in its response.[41] While discussing specific and technical responses to cyberattacks with offensive cyber capabilities may be challenging, a general discussion of tools available to the U.S. government and conditions under which certain tools may be deployed is not. The National Cyber Director, Chris Inglis, acknowledged the importance of all instruments of national power when bringing accountability to cyberspace, as well as the utility of the National Security Council in coordinating those tools:[42]

> The role of the national security council, which outside of cyberspace is accountable to use all the instruments of power that this nation can bring to bear—diplomacy, intelligence, military resources, financial resources, sanctions that might be applied—to bring about the proper conditions in all domains, not least of which [is] cyberspace.

Other governments have generally shown a willingness to more openly discuss options to respond to cyberattacks. The European Union (EU) developed the "Cyber Diplomacy Toolbox" to list and describe actions the EU may take in response to cyberattacks, depending on the level of confidence in attribution a victim member state has in the perpetrator, and the level of

[38] P.L. 114-113, Division N, §402.

[39] Executive Office of the President, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Federal Register* 22391-22397, May 11, 2017.

[40] For examples, see the following: Department of State, "Department of State International Cyberspace Policy Strategy," March 2016, at https://2009-2017.state.gov/documents/organization/255732.pdf; Department of State, "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," May 31, 2018, at https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf; and Department of State, Recommendations to the President on Protecting American Cyber Interests through International Engagement," May 31, 2018, at https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf.

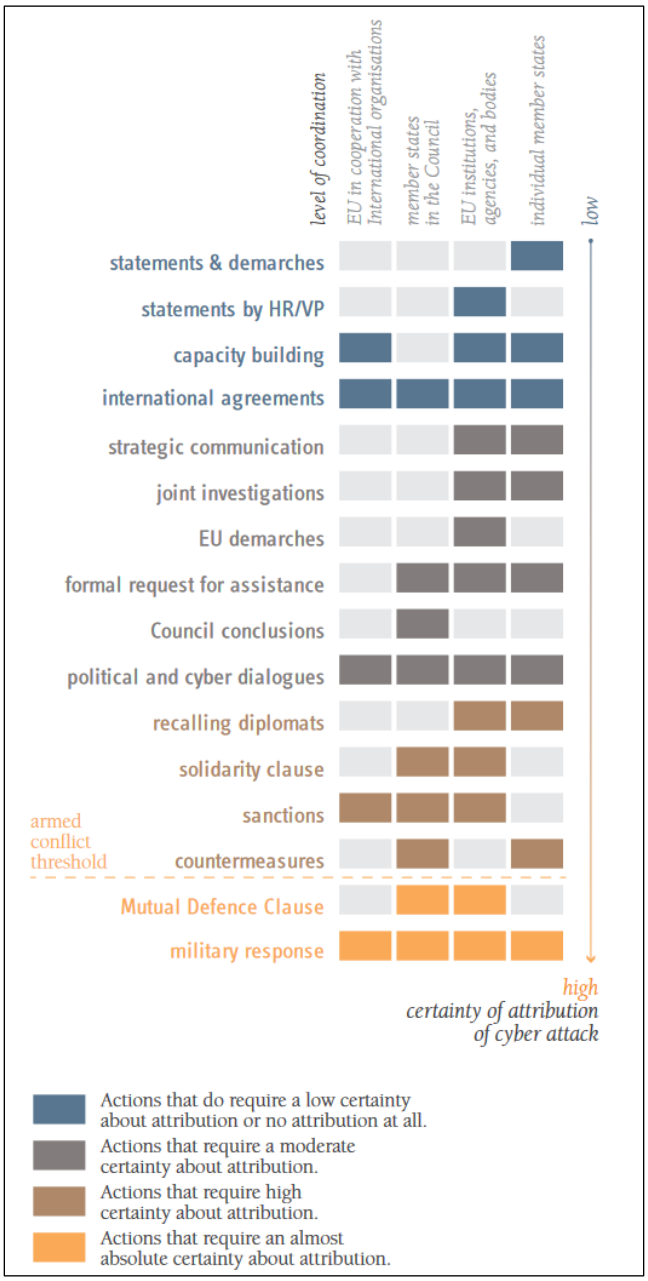
[41] CSIS, "Discussing the UN OEWG with the Mother of Norms," Inside Cyber Diplomacy podcast, March 26, 2021, at https://www.csis.org/podcasts/inside-cyber-diplomacy.

[42] U.S. Congress, House Committee on Oversight and Reform, *Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats*, 117th Cong., 1st sess., November 16, 2021.

coordination necessary to effectively implement the action. **Figure 2** list the actions in the Cyber Diplomacy Toolbox. The policy is still relatively new and how the EU chooses to adhere to it in the future remains to be seen. Key elements to response certainty include having stated consequences to cyberattacks and reliably executing the actions that deliver those consequences.

Figure 2. European Union Cyber Diplomacy Toolbox Actions

By Attribution Confidence



Source: Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?" *European Union Institute for Security Studies*, July 2017, at https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

Notes: European Union (EU). High Representative for the Union for Foreign Affairs and Security Policy (HR/VP).

The existence of potential response options a nation may employ against cyberattack perpetrators need not bind that nation only to those options. As a deterrence tool, stated options can create potential fear of reprisal on the part of the attacker. Discussions on which tools may be publicly disclosed as possible responses presents an opportunity to engage the international community in norms-setting activities and developing normative behavior. Both may provide paths for increased stability in cyberspace.[43]

Options for Congress

Over the past two years, the number of denial recommendations made by the Commission and acted upon by Congress or the President has outpaced those for dedicated deterrence activities. As discussed in "Deterrence Factors," Congress and the President have a history of pursuing and implementing strategies of denial to achieve cybersecurity.

Outstanding policy recommendations related to deterrence include

- Creating a bureau in the U.S. Department of State (nearing implementation);
- Strengthening norms of responsible state behavior in cyberspace (on track);
- Engaging in international standards setting fora (on track);
- Improving capability building and foreign assistance financing (on track);
- Developing confidence building measures (delayed);
- Leveraging sanctions and trade enforcement actions (on track); and
- Improving attribution (delayed).

These recommendations are further discussed below. Policymakers may choose to examine options to deter cyberattacks by creating government agencies to specifically address deterrence policy with allies and adversaries, advocating for the development and adoption of international norms and standards, and maturing certainty of response options.

New State Bureau

The Commission identified a challenge with addressing cyberattacks in the U.S. government; namely, that government activities are federated.[44] That is to say that agencies are independently authorized and it is at the Executive Office of the President where agency activities are regularly coordinated. The Commission recommended the creation of a National Cyber Director within the Executive Office of the President to oversee interagency activities related to national cybersecurity, which was enacted through the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.[45]

Another Commission recommendation relates to the creation of a bureau within the State Department to address cyberspace issues. Such a bureau was initiated during the Trump

[43] International Security Advisory Board, "A Framework for International Cyber Stability," report, July 2, 2014, at https://2009-2017.state.gov/documents/organization/229235.pdf.

[44] For examples, see the following: U.S. Government Accountability Office, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629, September 22, 2020, pp. 42-56, https://www.gao.gov/assets/gao-20-629.pdf; and Cyberspace Solarium Commission, *Final Report*, Washington, DC, March 2020, pp. 142-143.

[45] P.L. 116-283, §1752. 6 U.S.C. §1500.

Administration—the Cyberspace Security and Emerging Technologies Bureau[46]—to lead U.S. government diplomatic efforts on cybersecurity. The Government Accountability Office (GAO) found that its establishment was hasty and its responsibilities and relationships were ill-defined.[47] The Biden Administration halted progress on the bureau until October 2021. Secretary Blinken has since announced the creation of two new positions at the State Department to address cyber and digital concerns.[48] The first would be an ambassador-at-large heading the Bureau of Cyberspace and Digital Policy, and would focus on cybersecurity deterrence, policy, and negotiations. The second would be a Special Envoy for Critical and Emerging Technology, and would be responsible for coordinating policy with partner nations on artificial intelligence, quantum computing, and other technology-related fields. These developments came after the House of Representatives passed the Cyber Diplomacy Act of 2021 (H.R. 1251) authorizing a Bureau of International Cyberspace Policy.[49]

As Congress and the Administration advance plans to create a unit within the State Department focused on cyber issues, there remain outstanding concerns that policymakers may choose to address and conduct oversight on. GAO found that the State Department did not coordinate with other federal agencies during their first effort to create a bureau, and recommended it do so going forward.[50] Other agencies play a substantial role in international discussions on cyber norms and standards, engage in operations with partner nations, and house expertise on technical matters related to cyberspace. Should the State Department proceed with independently forming and empowering a bureau, the potential for policy fragmentation and duplication of efforts may compound.[51]

Largely unaddressed in previous efforts to create a new bureau in State is how it would engage with partner nations (e.g., EU member states), multinational bodies researching cybersecurity (e.g., NATO's Cooperative Cyber Defence Centre of Excellence),[52] or civil society efforts related to cybersecurity norm building (e.g., the Paris Call).[53] Engaging in these types of international fora provides opportunities for the United States to lead policy development and model desirable behaviors for cyberspace engagement and operations.

[46] U.S. Department of State, "Secretary Pompeo Approves New Cyberspace Security and Emerging Technologies Bureau," press release, January 7, 2021, at https://2017-2021.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau/index.html.

[47] U.S. Government Accountability Office, *Cyber Diplomacy; State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies*, GAO-21-266R, January 28, 2021, https://www.gao.gov/products/gao-21-266r.

[48] Dustin Volz, "State Department to Form New Cyber Office to Face Proliferating Global Challenges," *Wall Street Journal*, October 25, 2021, at https://www.wsj.com/articles/state-department-to-form-new-cyber-office-to-face-proliferating-global-challenges-11635176700.

[49] Passed the U.S. House of Representatives on April 20, 2021.

[50] CRS In Focus IF10541, *Defense Primer: Ballistic Missile Defense*, by Stephen M. McCall; U.S. Government Accountability Office, *Priority Open Recommendations: Department of State*, GAO-21-457pr, May 19, 2021, pp. 3-4, https://www.gao.gov/assets/gao-21-457pr.pdf.

[51] Ibid.

[52] North Atlantic Treaty Organization, "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise," webpage, at https://ccdoe.org.

[53] Paris Call for Trust and Security in Cyberspace, "Paris Call" webpage, at https://pariscall.international/en.

International Norms and Standard Setting

Two Commission recommendations address cybersecurity norms: one discusses advancing norms and the other makes suggestions around engaging international bodies on ICT standards development. These activities have the potential for the United States to model behaviors and lead the development of international order and ICT operations.

To some extent, the United States engages in these activities today. The State Department's Office of the Coordinator for Cyber Issues (S/CCI)[54] worked on developing the 11 norms of responsible state behavior in cyberspace and many federal agencies participate in international standards development activities.[55]

Should policymakers choose to pursue options to advance international norms and/or the strengthening of the United States' role in norms setting, there are both existing and new opportunities to do so. Congress may choose to direct an agency to coordinate federal activities on norms setting, or provide expertise to another agency to inform norms development and advancement activities. This is commonly done for other cybersecurity activities today. For example, the Cybersecurity Act of 2015 (P.L. 114-113, Division N)[56] directed the Secretary of Homeland Security to establish a voluntary information sharing program with the private sector, but also directed the Secretary to work with the Attorney General on the procedures for participating in the information sharing program.

Congress may also choose to direct an agency to engage in norms setting fora. Despite the existence of 11 norms of responsible state behavior in cyberspace, opportunities exist to advance these principles, advance scholarship on norms, and engage nongovernmental groups on the norms. For example, two civil society groups are working on achieving peace in cyberspace—the Global Commission on the Stability of Cyberspace[57] and the Paris Call for Trust and Security in Cyberspace (Paris Call).[58] The North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defence Centre of Excellence,[59] develops scholarship on cyberspace operations. Among private sector stakeholders, the Microsoft Corporation has called for government and the private sector to work together to build new norms for cyber operations, akin to the Geneva Convention.[60] U.S. agency participation in these efforts provides an opportunity for the United States to drive norm-setting activities and influence the debate.

Policymakers may also choose to have agencies engage in new activities. For example, CISA has a strategy for engaging with national governments on securing the cyberspace.[61] Congress may

[54] For more information, see https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/.

[55] National Institute of Standards and Technology, "NIST Summary of the Responses to the National Science and Technology Council's Sub-Committee on Standards Request-for-Information, issued December 8, 2010: Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors," document, May 13, 2011, at https://www.nist.gov/system/files/documents/standardsgov/RFI-Summary-5-13-final2.pdf.

[56] 6 U.S.C. §§1501-1510.

[57] Global Commission on the Stability of Cyberspace, at https://cyberstability.org/.

[58] Paris Call for Trust and Security in Cyberspace, at https://pariscall.international/en/.

[59] North Atlantic Treaty Organization, "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise," webpage, at https://ccdoe.org.

[60] Brad Smith, "The Need for a Digital Geneva Convention," blog post, February 14, 2017, at https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[61] Cybersecurity & Infrastructure Security Agency, "CISA Global," document, February 17, 2021, at https://www.cisa.gov/sites/default/files/publications/CISA_Global_Print-021721_508.pdf.

choose to codify in law these activities and further direct CISA, or another agency like the National Institute of Standards and Technology (NIST) or the National Telecommunications and Information Administration (NTIA), to assist in ongoing norms and standards setting activities by providing technical expertise.

Options to Mature Response Capabilities

U.S. policymakers may choose to pursue a strategy of declaratory actions to deny or deter cyberattacks. The Commission made recommendations concerning attribution and use of sanctions, which may be additions to a matured response. If Congress chooses to pursue a strategy of stated and certain actions, there are existing options for activities to be outlined and described.

Congress may request that a declaratory policy be included as part of the National Security Strategy.[62] Congress may also request this information as part of the National Cyber Strategy.[63] Additionally, Congress may choose to make this request independent of existing strategy documents and task an agency or the National Cyber Director with producing the federal government's list of response actions to cyberattacks. In doing so, Congress may create an additional opportunity to conduct oversight of these activities and inquire as to how often they are being used and how effective they are at deterring cyberattacks. Congress recently requested that the Secretary of Defense provide a taxonomy of cyber capabilities.[64] Such a taxonomy may serve as a model for a fuller report on broader deterrence capabilities.

Conclusion

Deterring adversarial actions in cyberspace remains challenging. There are nuances to cyberspace that complicate the ability to apply current deterrence concepts to cyberattacks. Regardless of these challenges, many regard efforts to deter cyberattacks as a necessary step to achieve stable cyberspace operations. Establishing norms, having a way to detect violations, and developing reputable options to respond to attacks all contribute to a strategy of deterrence.

[62] P.L. 99-433, §603; 50 U.S.C. §3043. The National Security Strategy is released and sent to Congress annually.

[63] P.L. 116-283, §1752; 6 U.S.C. §1500. Statute is silent on the frequency that the National Cyber Strategy shall be sent to Congress, but the National Cyber Director is to report annually to Congress on the implementation of the strategy and the nation's cybersecurity posture.

[64] S. 1605, §1501.

Appendix. Cyberspace Solarium Commission Recommendations

Table A-1 contains the 109 recommendations from the Commission and their status.[65] Each recommendation in the table is categorized as either a deterrence or denial (or both) activity based on the definitions set forth in this report. There are five options for the assessed status of a recommendation:

- *Implemented* recommendations have been enacted by legislation, executive action, or agency activity;
- *Nearing Implementation* recommendations are in legislation or executive action that have a clear path to approval;
- *On Track* recommendations are partially implemented or are being considered. In many cases, the Commission has drafted an Executive Order or bill to address these recommendations, but the recommendation has not been formally considered;
- *Delayed* recommendations have not been rejected but do not have a policy action or vehicle for implementation; and
- *Significant Barriers* recommendations have received significant pushback from policymakers or have been outright rejected.

Table A-1. Cyberspace Solarium Commission Recommendations

Ascending by Pillar and Recommendation Identifier

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
Reform the U.S. Government's Structure and Organization for Cyberspace	1.1	Issue and Update National Cyber Strategy	In Process	Nearing Implementation	Both
	1.1.1	Develop a Multitiered Signaling Strategy	Executive Action Needed	On Track	Deny
	1.1.2	Promulgate a New Declaratory Policy	Executive Action Needed	Delayed	Deny
	1.2	Create House Permanent Select and Senate Select Committees on Cybersecurity	Faces Significant Barriers to Implementation	Significant Barriers	Both
	1.2.1	Reestablish the Office of Technology Assessment	Appropriations Needed	On Track	Both
	1.3	Establish National Cyber Director (NCD)	Legislation Passed in FY2021 NDAA, NCD Confirmed, Related E.O. Issued, Appropriated	Implemented	Both

[65] Statuses are as of December 20, 2021.

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	1.4	Strengthen the Cybersecurity and Infrastructure Security Agency	Legislation Passed in FY2021 NDAA, Related E.O. Issued	Implemented	Deny
	1.4.1	Codify and Strengthen the Cyber Threat Intelligence Integration Center	Legislation Proposed, Appropriations Needed	Delayed	Both
	1.4.2	Strengthen the FBI's Cyber Mission and National Cyber Investigative Joint Task Force	Appropriations Needed	On Track	Both
	1.5	Diversify and Strengthen the Federal Cyberspace Workforce	Partial Implementation via Legislation Passed in the FY2021 NDAA, Further Legislation and Appropriations Needed	On Track	Both
	1.5.1	Improve Cyber-Oriented Education	Appropriations Needed	Implemented	Deny
Strengthen Norms and Nonmilitary Tools	2.1	Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State	Legislation Engrossed	Nearing Implementation	Deter
	2.1.1	Strengthen Norms of Responsible State Behavior in Cyberspace	Executive Actions Taken, E.O. Proposed	On Track	Deter
	2.1.2	Engage Actively and Effectively in Forums Setting International ICT Standards	Legislation Engrossed, Appropriations Needed	On Track	Deter
	2.1.3	Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance	Legislation Proposed, Appropriations Needed	On Track	Deter
	2.1.4	Improve International Tools for Law Enforcement Activities in Cyberspace	Legislation Proposed, Appropriations Needed	Nearing Implementation	Both
	2.1.5	Leverage Sanctions and Trade Enforcement Actions	Legislation Proposed	On Track	Deter

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	2.1.6	Improve Attribution Analysis and the Attribution-Decision Rubric	E.O. Proposed	Delayed	Deter
	2.1.7	Reinvigorate Efforts to Develop Cyber Confidence-Building Measures	E.O. Proposed	Delayed	Deter
Promote National Resilience	3.1	Codify Sector-Specific Agencies and Sector Risk Management Agencies and Strengthen their Ability to Manage Critical Infrastructure Risk	Legislation Passed in the FY2021 NDAA	Implemented	Deny
	3.1.1	Establish a National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy	E.O. Proposed, Legislation Engrossed	Nearing Implementation	Deny
	3.1.2	Establish a National Cybersecurity Assistance Fund	Legislation Proposed	On Track	Deny
	3.2	Develop and Maintain Continuity of the Economy Planning	Legislation Passed in the FY2021 NDAA; Appropriations Needed	Implemented	Deny
	3.3	Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recover Fund"	Legislation Passed in the IIJA	Implemented	Deny
	3.3.1	Designation Responsibility for Cybersecurity Services Under the Defense Production Act	Faces Significant Barriers to Implementation	Significant Barriers	Deny
	3.3.2	Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts	Legislation Proposed	Delayed	Deny
	3.3.3	Improve and Expand Planning Capacity and Readiness for Cyber Incidence Response and Recovery Efforts	E.O. Proposed	On Track	Deny
	3.3.4	Expand Coordinated Cyber Exercises, Gaming, and Simulation	Appropriated	Implemented	Both

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	3.3.5	Establish a Biennial National Cyber Tabletop Exercise	Legislation Passed in the FY2021 NDAA	Implemented	Deny
	3.3.6	Clarify the Cyber Capabilities and the Interoperability of the National Guard	Legislation Passed in the FY2021 NDAA	Implemented	Both
	3.4	Improve the Structure and Enhance Funding of the Election Assistance Commission	Legislation Engrossed	On Track	Deny
	3.4.1	Modernize Campaign Regulations to Promote Cybersecurity	Legislation Proposed	On Track	Deny
	3.5	Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations	Legislation Proposed	Delayed	Deny
	3.5.1	Reform Online Political Advertising to Defend Against Foreign Influence in Elections	Legislation Proposed	On Track	Deny
Reshape the Cyber Ecosystem Towards Greater Security	4.1	Establish and Fund a National Cybersecurity Certification and Labeling Authority	Legislation Proposed, Related E.O. Issued	On Track	Deny
	4.1.1	Create or Design Critical Technology Security Centers	Appropriations Needed, Legislation Proposed	On Track	Deny
	4.1.2	Expand and Support NIST's Security Work	Legislation Proposed, Appropriations Needed	Delayed	Deny
	4.2	Establish Liability for Final Good Assemblers	Faces Significant Barriers to Implementation	Significant Barriers	Deny
	4.2.1	Incentivize Timely Patch Implementation	Appropriations Needed	On Track	Deny
	4.3	Establish a Bureau of Cyber Statistics	Legislation Proposed	On Track	Both
	4.4	Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications	Partial Implementation via Legislation Passed in the FY2021 NDAA	On Track	Deny
	4.4.1	Establish a Public-Private Partnership on Modeling Cyber Risk	E.O. Proposed	On Track	Both

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	4.4.2	Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events	Partial Implementation via Legislation Passed in the FY2021 NDAA	On Track	Both
	4.4.3	Incentivize IT Security Through Federal Acquisition Regulations and Federal Information Security Management Act Authorities	Implemented via E.O.	Implemented	Deny
	4.4.4	Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements	Legislation Proposed	On Track	Deny
	4.5	Develop a Cloud Security Certification	Executive or Legislative Action Needed	On Track	Deny
	4.5.1	Incentivize the Uptake of Secure Cloud Services for SMB and SLTT Governments	Legislation Introduced	On Track	Deny
	4.5.2	Develop a Strategy to Secure Foundational Internet Protocols and Email	Partially Implemented in the FY2021 NDAA	Nearing Implementation	Deny
	4.5.3	Strengthen the U.S. Government's Ability to Take Down Botnets	Legislation Introduced	On Track	Both
	4.6	Develop and Implement an ICT Industrial Base Strategy	In Process	Nearing Implementation	Deny
	4.6.1	Increase Support to Supply Chain Risk Management Efforts	Partial Implementation	On Track	Both
	4.6.2	Commit Significant and Consistent Funding toward R&D in Emerging Technologies	Partial Implementation	On Track	Deny
	4.6.3	Strengthen the Capacity of the Committee on Foreign Investment in the United States	Appropriations Needed	Delayed	Both
	4.6.4	Invest in the National Cyber Moonshot Initiative	Appropriations Needed	On Track	Deny
	4.7	Pass a National Data Security and Privacy Protection Law	Faces Significant Barriers to Implementation	Significant Barriers	Deny

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	4.7.1	Pass a National Breach Notification Law	Legislation Proposed	On Track	Both
Operationalize Cybersecurity with the Private Sector	5.1	Codify the Concept of "Systemically Important Critical Infrastructure"	Legislation Introduced	On Track	Both
	5.1.1	Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector	Legislation Proposed	On Track	Deny
	5.1.2	Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities	Legislation Proposed	On Track	Deny
	5.1.3	Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities	Legislation Passed in the FY2021 NDAA	Implemented	Both
	5.2	Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information	Legislation Proposed, E.O. Issued	On Track	Both
	5.2.1	Expand and Standardize Voluntary Threat Detection Programs	E.O. Proposed	On Track	Deny
	5.2.2	Pass a National Cyber Incident Reporting Law	Legislation Introduced	Nearing Implementation	Both
	5.2.3	Amend the Pen Register Trap and Trace Statute to Enable Better Identification of Malicious Actors	Legislation Proposed	On Track	Deny
	5.3	Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers	Legislation Passed in the FY2021 NDAA	Implemented	Both
	5.4	Establish a Joint Cyber Planning Cell in CISA	Legislation Passed in the FY2021 NDAA	Implemented	Deny
	5.4.1	Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives	Legislation Passed in the FY2021 NDAA	Implemented	Both

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	5.4.2	Expand Cyber Defense Collaboration with ICT Enablers	Executive Action Required	On Track	Deny
Preserve and Employ Military Instruments of Power	6.1	Direct DOD to Conduct a Force Structure Assessment of the Cyber Mission Force	Legislation Passed in the FY2021 NDAA	Implemented	Both
	6.1.1	Direct DOD to Create a Major Force Program Funding Category for U.S. Cyber Command	Partially Implemented via FY2021 NDAA	Nearing Implementation	Both
	6.1.2	Expand Current Malware Inoculation Initiatives	Executive Action Required	Delayed	Deny
	6.1.3	Review Delegation of Authorities for Cyber Operations	Legislation Passed in the FY2021 NDAA	Implemented	Both
	6.1.4	Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces	E.O. Proposed	Delayed	Both
	6.1.5	Cooperate with Allies and Partners to Defend Forward	E.O. Proposed	Nearing Implementation	Both
	6.1.6	Require DOD to Define Reporting Metrics	Legislation Required	On Track	Deny
	6.1.7	Assess the Establishment of a Military Cyber Reserve	Legislation Passed in the FY2021 NDAA	Implemented	Both
	6.1.8	Establish Title 10 Professors in Cyber Security and Information Operations	Executive Action or Legislation Required	Delayed	Both
	6.2	Conduct Cybersecurity Vulnerability Assessment of All Segments of the NC3 and NLCC Systems and Continually Assess Weapon Systems' Cyber Vulnerabilities	Legislation Passed in the FY2021 NDAA	Implemented	Deny
	6.2.1	Require DIB Participation in a Threat Intelligence Sharing Program	Partially Implemented via FY2021 NDAA	Nearing Implementation	Deny
	6.2.2	Require Threat Hunting on DIB Networks	Partially Implemented via FY2021 NDAA	Nearing Implementation	Deny

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	6.2.3	Designate a Threat-Hunting Capability Across the DODIN	Executive Action Required	Delayed	Deny
	6.2.4	Assess and Address the Risk to National Security Systems Posed by Quantum Computing	Legislation Passed in the FY2021 NDAA	Implemented	Deny
Cybersecurity Lessons from the Pandemic	PAN1.1	Provide SLTT Government and SMB IT Modernization Grants	Partially Implemented in the IIJA	Nearing Implementation	Deny
	PAN1.2	Pass an Internet of Things Security Law	Partially Implemented in the FY2021 NDAA	On Track	Deny
	PAN1.3	Support Nonprofits that Assist Law Enforcement's Cybercrime and Victim Support Efforts	Legislation Proposed	Delayed	Deny
	PAN1.4	Increase NGO Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns	Legislation Proposed	Delayed	Both
	PAN1.4.1	Establish the Social Media Data and Threat Analysis Center	Authorized	Nearing Implementation	Both
National Cyber Director	NCD1	Establish and National Cyber Director	Legislation Passed in the FY2021 NDAA	Implemented	Both
Growing a Stronger Federal Cyber Workforce	WF1	Establish Leadership and Coordination Structures	E.O. Proposed	Delayed	Both
	WF2	Properly Identify and Utilize Cyber-Specific Occupational Classifications	E.O. Proposed	Delayed	Both
	WF3	Develop Apprenticeships	Legislation Introduced	On Track	Both
	WF4	Improve Cybersecurity for K-12 Schools	Legislation Passed	Implemented	Deny
	WF5	Provide Work-Based Learning via Volunteer Clinics	E.O. Proposed	Delayed	Deny
	WF6	Improve Pay Flexibility/Hiring Authority	E.O. Proposed	Delayed	Both
	WF7	Incentivize Cyber Workforce Research	Legislation Proposed	On Track	Both

Pillar	Rec. #	Recommendation	Status	Assessment	Deter or Deny
	WF8	Mitigate Retention Barriers and Invest in DEI in Recruiting	Legislation Proposed	Delayed	Both

Building a Trusted ICT Supply Chain	SC1	Develop and Implement an ICT Industrial Base Strategy	In Process	Nearing Implementation	Deny
	SC2	Identify Key ICT technologies and materials	In Process	Nearing Implementation	Deny
	SC3	Conduct a Study on the Viability of and Designate Critical Technology Clusters	Legislation Engrossed	Nearing Implementation	Deny
	SC3.1	Provide R&D Funding for Critical Technologies	Appropriations Needed	On Track	Deny
	SC3.2	Incentivize the Movement of Critical Chip and Technology Manufacturing out of China	Legislation Proposed	On Track	Both
	SC3.3	Conduct a Study on a National Security Investment Corporation	Legislation Proposed	On Track	Deny
	SC4	Designate a Lead Agency for ICT Supply Chain Risk	In Process	Nearing Implementation	Deny
	SC4.1	Establish a National Supply Chain Intelligence Center	Legislation Proposed	On Track	Both
	SC4.2	Fund Critical Technology Security Centers	Legislation Proposed	On Track	Deny
	SC5	Incentivize Open and Interoperable Standards and Release More Mid-Band Spectrum	Executive Action Needed	Delayed	Both
	SC5.1	Develop a Digital Risk Impact Assessment for International Partners for Telecommunications Infrastructure Projects	Executive Action Needed	On Track	Deny
	SC5.2	Ensure That the EXIM, DFC, and USTDA Can Compete with Chinese State-Owned and State-Backed Enterprises	Legislation Proposed	On Track	Deny
	SC5.3	Develop a List of Contractors and Vendors Prohibited from Implementing Development Projects	Legislation Proposed	On Track	Deny

Source: CRS analysis of Cyberspace Solarium Commission, "2021 Annual Report on Implementation," report, August 2021, at https://drive.google.com/file/d/19V7Yfc5fvEE6dGIoU_7bidLRf5OvV2__/view.

Notes: The following abbreviations are used in the table: National Cyber Director (NCD); Fiscal Year (FY); National Defense Authorization Act (NDAA); Executive Order (E.O.); Infrastructure Investment and Jobs Act (IIJA, P.L. 117-58); National Institute of Standards and Technology (NIST); Information Technology (IT); Small and Medium-Sized Businesses (SMB); State, Local, Tribal, and Territorial (SLTT); Information and Communications Technology (ICT); Research and Development (R&D); Cybersecurity and Infrastructure Security Agency (CISA); Department of Defense (DOD); Nuclear Command, Control, and Communications (NC3); National Leadership Command Capabilities (NLCC); Defense Industrial Base (DIB); DOD Information Network (DODIN); Nongovernmental Organization (NGO); Diversity, Equity, and Inclusion (DEI); Export-Import Bank of the United States (EXIM); U.S. International Development Finance Corporation (DFC); and United States Trade and Development Agency (USTDA).

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer