CYBER RED LINES

Government Responses to Cyberattacks on Critical Infrastructure

Denise L. Tennant
Louis Nolan
Deanna House

While the concept of red lines is relatively well-documented and discussed in areas of research surrounding deterrence and acts of war, the term *cyber red lines* is rather complicated and fairly immature in the research. Recognizing the ongoing challenges surrounding the red line term in a cyber context, this article seeks to define such a threshold within gray-zone cyber operations to determine an appropriate situation when the US Department of Defense could and should respond to state or nonstate actor operations that manifest as a cyberattack. The article also seeks to clarify what is meant by the term *cyber gray zone*.

Research surrounding red lines in terms of great power conflict and war provides an important area of study in order to understand what defines a red line and how it can be influential to conflict.[1] Red lines within a cyber context, however, are not as clearly articulated and represent an evolving concept with many complicated nuances. The amorphous nature of the cyberspace domain—unlike the air, land, sea, and even space domains—and the vaguely understood boundaries between US and adversary cyber terrain can prove problematic when drawing cyber red lines.

Furthermore, the ubiquitous nature of technology, and more specifically cyber-related technology, can create challenges in understanding and determining the role of the Department of Defense in response to offensive cyberspace operations (CO) by state and nonstate actors. Joint doctrine defines cyberspace operations as "the employment

Denise Tennant is deputy chief of operations of the Information Effect Directorate, Joint Warfare Analysis Center, in Dahlgren, Virginia, and holds a juris doctor from the Marshall-Wythe School of Law at the College of William and Mary.

Louis Nolan is a Department of the Air Force civilian at United States Strategic Command, Offutt Air Force Base, Nebraska, and holds a master of science in systems management from the University of Southern California.

Dr. Deanna House is an assistant professor of information systems and quantitative analysis, co-director of the Nebraska Deterrence Lab at the College of Information Science and Technology, and Cyber Threat Analysis Lab research lead, National Counterterrorism Innovation, Technology and Education Center, University of Nebraska Omaha.

1. See, for example, Thomas G. Mahnken and Gillian Evans, "Ambiguity, Risk, and Limited Great Power Conflict," *Strategic Studies Quarterly* 13, no. 4 (2019), https://www.airuniversity.af.edu/; and Derek Grossman and Joel Speed Meyers, "Minding the Gaps: US Military Strategy toward China," *Strategic Studies Quarterly* 13, no. 4 (2019).

of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" and includes not only military and intelligence but also DoD business components. Importantly, cyberspace operations can be malicious but are not always so.[2]

In the era of technological advancements, identifying strategic inflection points—points at which businesses or organizations undertake significant changes in order to remain competitive—is critical.[3] In the case of cyber strategic inflection points for the military, this means a move to develop capabilities superior to that of an adversary. Efforts to identify current cyber strategic inflection points and motivations that drive change create ongoing challenges surrounding when the Defense Department could and should respond to state or nonstate actor operations that manifest as a cyberattack.

Response to a cyberattack that results in an escalation beyond the virtual realm would typically not occur due to the nonphysical nature of attacks and their temporary and reversible effects.[4] The relationship between deterrence and red lines can be complicated in cyber-specific engagements, mainly due to attribution and to challenges surrounding capabilities.

In instances of cyberattacks, it can be difficult to know whether an attack will be effective due to the ever-changing network and software environment. Attribution can be hard to attain when responding to a cyberattack. Raising false flags and taking time to examine an attack forensically to determine its origin can prevent a swift response.[5] In addition, traditional deterrence methods that involve disclosing specific details about capabilities can provide adversaries with information that could result in preventing or deflecting an attack.[6] This article thus explores the concept of cyber red lines and provides a starting point for understanding what this means in terms of responses to cyberspace operations conducted by adversary state and nonstate actors.

In order to establish a baseline understanding of cyber red lines, this article relies heavily on legal and academic literature analyzing the current state of international law and norms applicable to cyberspace, official US policy documents on cyberspace and cyberspace operations, and proposed cybersecurity approaches, as well as on news reports and academic analyses of these operations.

---

2. *Joint Cyberspace Operations*, Joint Publication (JP) 3-12 (Washington, DC: Chairman of the Joint Chiefs of Staff, December 19, 2022), I-1.

3. Robert A. Burgelman and Andrew S. Grove, "Strategic Dissonance," *California Management Review* 38, no. 2 (1996), https://doi.org/.

4. Erica Borghard and Shawn W. Lonergan, "Public-Private Partnerships in an Era of Great-Power Competition," in "Ten Years In: Implementing Strategic Approaches to Cyberspace," *Newport Papers* 45 (2020), https://digital-commons.usnwc.edu/.

5. Joseph F. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016), https://doi.org/.

6. Davi M. D'Agostino et al., *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets*, GAO-10-147 (Washington, DC: Government Accountability Office, 2009), https://www.gao.gov/.

Defining Cyber Red Lines

This article defines a red line as the threshold at which an action taken is so grievous that a use of force in response would be generally accepted under international law. This definition sets the upper boundary for the gray zone, the nebulous area of actions that fall below the threshold of armed conflict but may still warrant a US government response. In this zone, cyberspace operations provide a unique context under which adversaries can hide activities, create uncertainty, and avoid attribution—all key components that blur the evidence that would warrant a use of force as a response.[7] Further defining the gray zone as it relates to CO and the thresholds for the DoD response to actions within it is part of the larger analytic focus of this article.

The term *red line* is frequently used, but in the case of cyber, it remains inadequately defined. The context-specific nature of cyberattacks creates an air of ambiguity surrounding consequences should a red line be crossed. There is rarely agreement on the term, with definitions ranging from "an expression used by governments to privately define a threshold for action" to "an unequivocal threat, a line in the sand that if crossed, the target would incur the full fury of the state that issued the threat in the first place."[8] This lack of common understanding creates an uncertainty that makes effective deterrence even more difficult.

The construct of red lines is prevalent in every continent with the number of red lines currently drawn at an all-time high.[9] Formal declarations of cyber red lines have made a recent appearance but remain vaguely developed and bring up the challenges in maintaining a state's moral credibility when responding to out-of-bounds attacks.[10]

The UN norms of responsible state behavior are intended to determine norms for appropriate cyber behavior in the interest of maintaining peace and security. Significant undertakings such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*—the 2013 academic manual that explored international law principles as they relate to cyber warfare and its 2017 follow up, respectively—also provide mechanisms for determining a starting point for behavior in the cyberspace domain.

7. Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020).

8. Bruno Tertrais, *The Diplomacy of "Red Lines": Recherches & Documents* (Paris: Fondation pour la Recherche Stratégique, February 1, 2016), https://www.frstrategie.org/; and Albert Wolf, "Backing Down: Why Red Lines Matter in Geopolitics," Modern War Institute, August 18, 2016, https://mwi.westpoint.edu/.

9. David Andelman, *A Red Line in the Sand: Diplomacy, Strategy, and the History of Wars That Might Still Happen* (New York: Pegasus Books, 2021).

10. Stephanie Pendino, Robert K. Jahn Sr., and Kirk Pedersen, "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light," *Campaigning: the Journal of the Joint Forces Staff College*, September 7, 2022, https://jfsc.ndu.edu/.

Yet existing norms are either lacking or still subject to debate, especially in strategic interstate competition short of armed conflict.[11]

Literature surrounding national security is replete with concerns about the establishment of red lines in general and cyber red lines in particular. One analysis of historical and current red lines, such as those drawn by China in the South China Sea that are "physical, diplomatic, military, [and] all too often existential," contends that such "lines in the sand" have "proliferated in recent years across every continent and . . . have reached a toxic apex in numbers and virulence at this very moment in history."[12] In pointing to their limitations, the analysis further notes that red lines work best only if both sides accept their parameters.[13] Moreover, an adversary can ignore a red line and force the United States to implement a response or action it does not desire to take. In a different vein, red lines can serve as a provocation, eliciting further activity as a psychological response to being told what not to do.[14]

In terms of establishing a cyber red line, an oft-cited concern is an adversary conducting gray-zone cyber actions that fall just below that line.[15] Additionally, as discussed above, it is not always possible to establish attribution with confidence and to act in a timely manner. Establishing norms for behavior that take the spectrum of cyberspace operations into consideration can be a useful starting point. The high-cost effects such as those targeting the general population that are physically destructive and potentially lethal and irreversible should be avoided on the offensive but also the defensive side.[16]

Yet establishing cyber red lines can have an advantage; the cyber red line argument is not one-sided. Lacking codified cyberspace international law or norms, red lines can address a void or gap within international law.[17] Despite some of the potential shortcomings noted above, the red line construct remains prevalent and can be useful to conceptually frame offensive cyberspace operations below the level of armed con-

11. Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013); Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge, UK: Cambridge University Press, 2017); Gary Corn, "Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, ed. Winston S. Williams and Christopher M. Ford (2018, forthcoming), https://papers.ssrn.com/; and Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (2017), https://doi.org/.

12. Andelman, *Red Line*, 1.

13. Andelman, *Red Line*.

14. Dan Altman and Kathleen E. Powers. "When Redlines Fail: The Promise and Peril of Public Threats," *Foreign Affairs*, February 2, 2022. https://www.foreignaffairs.com/.

15. Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022), 1, https://doi.org/.

16. Pendino, Jahn, and Pedersen, "Cyber Deterrence."

17. Andelman, *Red Line*.

flict.[18] Furthermore, red lines impact global perceptions of power and influence; research suggests the reputation of the United States may suffer if an adversary appears to cross a red line without generating an appropriate or implied response.[19]

Cyberspace Operations and the Cyber Domain

Securing information systems and technology to maintain continued operations of critical infrastructure (CI) is complicated due to the varying responsibilities of government and private sector entities. This is an ongoing and rapidly changing environment, with government-driven policies and compliance requirements offering guidance on how entities respond to attacks. Cybersecurity is vital to Americans' everyday lives, US society, and continued innovation. It is a must-succeed mission that supports the United States' survival as a sovereign nation. The United States must employ prudent measures to prevent adversaries from conducting cyberspace operations that cripple its ability to operate in the modern world and be prepared to respond appropriately if cybersecurity measures fail.

Attackers frequently target critical infrastructure, which can extend effects beyond that of a defense entity and could bridge the gap between the virtual and physical realms. Critical infrastructure, which includes both DoD and non-DoD assets and facilities, consists of "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters."[20] Examples of CI sectors include energy, dams, communications, and the defense industrial base. Reliance by the Department of Defense on CI could affect core missions and assets.

Cyberspace, a global domain within the information environment, complements the four physical DoD warfighting domains yet is distinct as both the public and private sectors operate ubiquitously in cyberspace and rely on civilian networks and infrastructures to conduct basic functions.[21] Some 90 percent of US critical infrastructure is operated by the private sector. The expanding reliance on small business technology firms, academic institutions, and federally funded research and development centers to conduct state-of-the-art research as part of the defense ecosystem

18. Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), https://doi.org/.

19. Altman and Powers, "When Redlines Fail."

20. Joseph R. Biden Jr., National Security Memorandum on Critical Infrastructure Security and Resilience, NSM-22, April 30, 2024, https://www.whitehouse.gov/.

21. JP 3-12.

frames the dependency on the private sector to advance and secure US society and its economic engine.[22]

Cyberspace operations against US critical infrastructure and other private sector businesses pose new challenges, but these cyberattacks and the appropriate responses to them must be considered within the framework of existing international law. The ability of states to respond to adversary CO in times of conflict is addressed by experts in international law, but uncertainty remains concerning when and how it is appropriate for the Department of Defense to respond in peacetime, particularly if the target is not military in nature.[23] The *Tallinn Manual 2.0* outlines the current understanding of international law surrounding state CO in peacetime but also identifies numerous areas where experts are not in agreement about what international law requires.[24]

As early as 1984, the opportunity to exploit data "from converging telecommunications and automated information systems" was seen as a risk to US security.[25] In 1995, cyber threats to the energy sector, one of the 16 CI sectors, foreshadowed an evolving, nonkinetic means to threaten the US homeland.[26] Applying the Cold War construct of nuclear deterrence, the US response to adversary CO, to include that against US critical infrastructure and private sector businesses, was couched in a "cyber deterrence" framework.[27] Yet scholars and practitioners found the approach to be too responsive, not proactive, and not effective as "adversary CO and campaigns targeting US interests over that period . . . increased in frequency, scope, scale, and sophistication."[28]

The Cyberspace Solarium Commission, the bipartisan intergovernmental organization established under the 2019 National Defense Authorization Act to determine a strategy for US cyberspace defense, devised the layered cyber deterrence approach to curtail the "probability and impact of cyberattacks of significant consequence" via the three complementary ways of shaping behavior, denying benefits, and imposing

22. Micah Zenko, "Reading between the Red Lines: Deterrence and US Foreign Policy," Lessons for History Series, Council on Foreign Relations, May 10, 2021, audio podcast and YouTube video, 04:51, https://www.cfr.org/; and Lloyd J. Austin III, *National Defense Strategy of the United States of America including the 2022 Nuclear Posture Review and the 2022 Missile Posture Review* (Washington, DC: Department of Defense, October 27, 2022), https://media.defense.gov/ .

23. Schmitt, *Tallinn Manual*.

24. Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 735, https://www.law.georgetown.edu/; and Schmitt, *Tallinn Manual 2.0*.

25. Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

26. Michael Warner, "A Brief History of Cyber Conflict," in "Ten Years In"; Barack Obama, Critical Infrastructure Security and Resilience, Presidential Policy Directive – 21 [PPD-21], February 12, 2013, https://obamawhitehouse.archives.gov/; and Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, "Preface," in "Ten Years In."

27. Libicki, *Crisis and Escalation*.

28. Schneider, Goldman, and Warner, "Preface," 45; and Michael P. Fischerkeller and Richard J. Harknett, *Initiative Persistence as the Central Approach for US Cyber Strategy*, IDA Document NS D-22719 (Alexandria, VA: Institute for Defense Analysis, 2021), https://www.ida.org/.

costs.[29] The move away from the traditional "response force"–focused concept—responding after an attack—and into offensive cyber capabilities is necessary to maintain effective cyber deterrence strategies.

This shift from response-force/defensive actions to an offensive approach necessitates understanding the term *persistent engagement*, which is defined as "a use of cyber capabilities in continuous contact with adversaries to generate tactical, operational, and strategic initiative (and thus set the conditions of security in our favor in a constantly changing domain)."[30]

In a similar manner, persistent engagement has also been referred to in the literature as initiative persistence, which has been proffered as the central focus for US national cyber strategy and is defined as "a strategic approach to preclude, mitigate, and counter strategically consequential cyber action occurring continuously short of armed conflict." It stresses the need to compete continuously—the crux of US Cyber Command's persistent engagement doctrine—in the gray zone of CO and not cede the domain to the adversary.[31] These concepts have emerged to fill the perceived void in US deterrence theory as applied to actions within the cyber gray zone.[32] In short, cyber conflict is ongoing and constant.

In terms of the current cyberspace terrain, the notion of a second strategic inflection point within the cyber domain is trending.[33] The first strategic inflection point occurred in 2013 when adversaries commenced "operat[ing] continuously against CI, government networks, defense industries, and academia—both in America and abroad."[34] After this point, there was a significant expansion when the cyber threat shifted from espionage and exploitation to disruption and data deletion.[35]

In 2020 the Cyberspace Solarium Commission's report highlighted a second strategic inflection point focused on adversaries' targeting of cyber and related technologies that "improve the quality of human life." Further, it noted that "threats continue to grow at an accelerating pace" and that "America is facing adversary nation-states, extremists, and criminals that are leveraging emerging technologies to an unprecedented degree."[36] This is driving the need for public-private partnerships when fighting adversaries.

Individual responses by private sector entities, however, are complicated by the Computer Fraud and Abuse Act—also referred to as the antihacking law—which prohibits any unauthorized access to a computer, either knowingly or unintentionally.[37] Conducting defensive activities that violate the act is considered illegal and

29. Angus King et al., *Report of the United States of America Cyberspace Solarium Commission* (Washington, DC: Cyberspace Solarium Commission, March 2020), https://cybersolarium.org/.
30. Schneider, Goldman, and Warner, "Preface," 45.
31. Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, 1.
32. Paul M. Nakasone, "A Cyber Force for Persistent Operations," in "Ten Years In."
33. Nakasone, "Persistent Operations," 45; and King et al., *Cyberspace Solarium*.
34. Nakasone, 45.
35. Schneider, Goldman, and Warner, "Preface," 45.
36. King et al., *Cyberspace Solarium*.
37. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986).

is a punishable offense. Thus, the private sector looks to government entities to assist with responding to activities that edge into areas of national security and defense. The recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 has further constrained the responsibilities of private sector entities to reporting only and places the onus of a response on the government.[38] In addition, adversary actions in the cyber domain are an increasing concern as a part of hybrid warfare, which includes conventional and unconventional tactics conducted by a spectrum of state and nonstate actors and blurred together in an uncharacterized fashion.[39]

While cyberspace is still a maturing domain, numerous case studies exist that explore the actors; the specific tactics, techniques, and procedures employed by the cyber attacker and during the subsequent response by the target; the impact to the target; and the ramifications for cyber norms.[40] One example focuses on Russia's alleged cyberattack on US government and private sector networks via the US information technology company SolarWinds.[41] Ransomware attacks on municipalities, health care facilities, and school systems and breaches of consumer data and potential release of personally identifiable information are routinely in the news. Recent attacks have trended toward critical infrastructure and have brought to light vulnerabilities that exist in the aging infrastructure of the United States.[42] Who and what organizations are best postured to respond to these cyberattacks is frequently debated. Which organization, acting within statutory constraints and in alignment with international law and norms, should be granted affirmative authority to conduct offensive cyberspace operations is also under debate.[43]

International Law and Cyberspace Operations

With so much uncertainty regarding what state conduct is permissible in the cyber domain, this article intentionally sets a high bar for crossing the cyber red line. Making a connection between the virtual and physical world is best understood in terms of effects and by taking into consideration what in the cyber world constitutes an attack that is equivalent

38. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity and Infrastructure Security Agency (CISA), accessed June 5, 2024, https://www.cisa.gov/.

39. Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), https://potomacinstitute.org/.

40. Faisal Quader and Vandana P. Janeja, "Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies," *Journal of Cybersecurity and Privacy* 1, no. 4 (2021), https://doi.org/; and Marcus Willett, "Lessons of the SolarWinds Hack," *Survival: Global Politics and Strategy* 63, no. 2 (2021), https://doi.org/.

41. Willett.

42. Raphael Satter, "US Warns Hackers Are Carrying Out Attacks on Water Systems," Reuters, March 20, 2024, https://www.reuters.com/; and Sophia Fox-Sowell, "'We Know They're on the Network,' CISA Official Says of Nation-State Actors Infiltrating U.S. Critical Infrastructure," StateScoop, March 19, 2024, https://statescoop.com/.

43. Corn, "Cyber National Security."

to a conventional attack.[44] The definition of a red line stated previously assumes there is a threshold accepted by the international community at which an armed attack using CO would warrant a permissible response of self-defense by the targeted state.

This section examines international law and norms as they apply to the use of force in general, and how they are understood to apply to actions in the cyber domain in particular. Cyberspace operations conducted by states that do not cross the cyber red line but are not recognized as permitted state activity under international law fall into the cyber gray zone. In recent years, the cyber gray zone has extended into commercial entities and civilian populations, further complicating and broadening the scope of permitted state activity.[45]

The United States has long recognized the applicability of existing international law to the cyber domain, acknowledging the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. [Instead,] long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[46] The primary body of international law regulating when states may use force—jus ad bellum—is rooted in the principles of sovereignty and nonintervention. Sovereignty includes the right of a state to control access to its territory and to exercise jurisdiction and authority on its territory.[47] The principle of nonintervention gives each state the right to conduct its own affairs without outside interference.[48] The two types of state practices that run afoul of the principles of sovereignty and nonintervention are the use or threat of "force" and the use of nonforceful but coercive intervention.[49]

The prohibition against the use or threat of force is found in article 2(4) of the UN Charter: "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[50] The UN Charter does not offer a definition of the use of force, nor has an authoritative definition been accepted by the in-

44. Ron Granieri and Patrick Walsh, "If-Then: Defining the Red Line in Cyberspace," April 19, 2022, in *A Better Peace: A War Room Podcast*, podcast, MP3 audio, 31:45, https://warroom.armywarcollege.edu/; and Catherine A. Theohary, "Use of Force in Cyberspace," In Focus (Washington, DC: Congressional Research Service, June 25, 2024), https://crsreports.congress.gov/.

45. Cassandra Steer, "International Humanitarian Law in the 'Grey Zone' of Space and Cyber," CIGI Essay Series: Cybersecurity and Outer Space, CIGI [Centre for International Governance Innovation], January 29, 2023, https://www.cigionline.org/.

46. Obama, PPD-21.

47. Schmitt, *Tallinn Manual.*

48. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), Judgment, 1986 I.C.J. Rep. 14 (June 27), https://www.refworld.org/.

49. Peter Z. Stockburger, "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum," *American University International Law Review* 31, no. 4 (2016), https://digitalcommons.wcl.american.edu/.

50. United Nations [UN] Charter, 1945, article 2(4), https://www.un.org/.

ternational community. The International Court of Justice has stated the prohibition on use of force applies to "any use of force, regardless of the weapons employed."[51]

The United States has long taken the position that the "inherent right of self-defense potentially applies against any illegal use of force . . . [and] there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[52]

The principle of nonintervention has recognized exceptions, but generally, intervening in a state's choice of a "political, economic, social and cultural system, and the formulation of foreign policy" is not permitted.[53] Yet, this is not a complete bar to state action, as states may still promote and encourage the fulfillment of self-determination rights within another state.[54]

International efforts to answer outstanding questions of how existing laws and norms apply to cyberspace resulted in the *Tallinn Manual* and are supplemented by the *Tallinn Manual 2.0*.[55] The rules set forth in these two manuals are an attempt by the so-named International Group of Experts to capture the current state of international law and norms but are nonbinding on states and may continue to evolve with changing national interests in cyberspace.

Scholarship has identified three main approaches for determining if a cyberspace operation crosses the threshold to be considered a use of force or armed attack under international law: an instrument-based approach, which looks at the form of weapon used and whether the attack possesses the physical characteristics traditionally associated with military coercion; the target-based approach, which treats any CO against critical infrastructure as an armed attack; and the effects-based approach, which focuses on the overall effects of the CO and considers factors such as severity, immediacy, and directness of harm.[56]

Taking the three approaches into consideration, cyberspace operations "constitute 'armed attack[s]' when they are aimed at causing irreversible disruption or physical damage to a cyber-physical system, which is a physical system monitored or controlled by computers."[57] The term *significant* is also an important consideration when identifying if damage from a cyberattack warrants a use of force.[58] But if the intended disruption or damage is trivial, or the cyberattack is aimed at causing disruption or damage to computers or networks that do not monitor or control physical systems,

51. "Legality of the Threat or Use of Nuclear Weapons. Overview of the Case," International Court of Justice, accessed June 5, 2024, https://www.icj-cij.org/.

52. Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (2012): 7, https://journals.law.harvard.edu/.

53. Nicar. v. US.

54. Stockburger, "Known Unknowns," 31.

55. Schmitt, *Tallinn Manual*; and *Tallinn 2.0*.

56. Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," *Joint Force Quarterly*, no. 67 (2012), https://ndupress.ndu.edu/; and Reese Nguyen, "Navigating Jus Ad Bellum in the Age of Cyber Warfare," *California Law Review* 101, no. 4 (2013): 1083–4, https://lawcat.berkeley.edu/.

57. Nguyen, 1084.

58. Akber Khan, "Deterrence and the Problem of Attribution in Cyberspace: An Analysis of Vulnerabilities and Options for Pakistan," *Balochistan Think Tank Network Journal* 1, no. 2 (2022): 6–7.

"the action could be considered an illegal 'use of force' or an 'armed attack' justifying responsive force, depending on the gravity of the intended or reasonably foreseeable consequences."[59] This approach has considerable merit, but as discussed below, it is incomplete without the consideration of several additional factors.

As mentioned, a recurring issue in the cyber domain is that of attribution—assigning responsibility for a CO to a state or nonstate actor. In the Nicaragua v. United States case, the International Court of Justice found that a state with "effective control" over nonstate actors is responsible for those acts, at least within the context of military operations.[60] The International Criminal Tribunal for the Former Yugoslavia adopted a different threshold of "overall control," requiring state participation in the planning and supervision of military operations.[61] In general, international law will find the conduct of a person or group of persons to be "considered an act of a state under international law if the person or group of persons were acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[62]

A discussion of international laws relating to cyberspace operations would be incomplete without mentioning the one specific type of operations that is not viewed as a violation of international laws and norms, namely espionage. Espionage, whether through traditional physical methods or through CO, is generally tolerated by the international community during peacetime, "because, among other things," it "can reduce the chance of a misunderstanding that could lead to a real conflict."[63] But recent attacks targeting critical infrastructure and those that seek to interfere with elections are becoming destructive enough to be considered cyber warfare and thus moving toward a cyber red line.[64]

The state that is the target of an espionage operation might rightly choose to respond with punitive measures, but ordinary cyberspace operations to conduct espionage are not included in this analysis. In the example of the SolarWinds attack, which had underlying goals of espionage, the appropriate response would be for the United States to make it difficult for Russia to conduct espionage but not expect it to be prevented entirely.[65]

Establishing Cyber Red Line Norms

Preventing and responding to the unique challenges of adversary actions in the cyber domain require a whole-of-nation investment. One part of the US strategy is integrated deterrence, which uses every tool at the Department of Defense's disposal

59. Nguyen, "Jus Ad Bellum," 1084.

60. Nicar. v. US.

61. Stockburger, "Known Unknowns," 31.

62. International Law Commission, "Responsibility of States for Internationally Wrongful Acts," in *International Documents on Environmental Liability*, ed. Hannes Descamps, Robin Slabbinck, and Hubert Bocken (Dordrecht, Netherlands: Springer Science + Business Media, 2008), https://link.springer.com/.

63. Willett, "SolarWinds Hack," 12.

64. Kevin Townsend, "NATO Draws a Cyber Red Line in Tensions with Russia," SecurityWeek, May 13, 2024, https://www.securityweek.com/.

65. Willett, "SolarWinds Hack," 20.

in close coordination across the US government and with Allies and partners to deter aggression by other states.[66] This involves integrating across military domains—land, air, maritime, space, and cyber—and nonmilitary domains, including economic, technological, and information.[67]

While the Department's role in defending against or responding to gray-zone cyberattacks against US critical infrastructure and other private sector businesses is becoming clearer, its appropriate response remains less clear. Within its eight Unified Command Plan mission areas, strategic deterrence is the logical avenue for addressing gray-zone cyberattacks, drawing upon integrated deterrence as a mechanism to combine capabilities across regions, domains, the spectrum of conflict, the US government and Allies and partners.[68]

Strategic deterrence entails far more than nuclear operations and nuclear deterrence. Particularly in situations where tensions are already heightened, cyberspace operations could contribute to a strategic deterrence failure. The role of strategic deterrence is to make the cost to adversaries high enough that they do not take military action against the United States, its national interests, and its Allies and partners. Considerations for understanding the intensity of gray-zone attacks can bridge the cyber-specific gap between strategic and integrated deterrence.

Conclusion

While a gray-zone cyberattack against US critical infrastructure or private sector businesses might not look like a traditional kinetic attack, the outcomes and harms from a cascading cyberattack could rapidly exceed the damage from one or even several conventional kinetic weapons. The importance of effects—such as irreversible damage—and attribution are key elements in understanding cyber red lines. This article provides a starting point for future academic research to examine the details of specific cyber operations to determine if these operations threatened the target state's "sovereignty, peace, and security."[69]

The International Group of Experts that created the *Tallinn Manual* and *Tallinn Manual 2.0* could not agree on what would constitute a cyber "armed attack," with some adopting an approach that limited it to physical effects and others supporting an approach that focused on the severity of the effects and did not require they be physical in nature.[70] Norms around the use of CO are still developing, leading to ambiguity in terms of what constitutes an attack that would warrant the use of force, much less the threat of force, in response as defined in international law.

---

66. Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: White House, October 2022), https://www.whitehouse.gov/; and King et al., *Cyberspace Solarium*.

67. Biden.

68. Biden; 2022 Unified Command Plan, Memorandum of the Secretary of Defense, 88 Fed. Reg. 26219 (January 13, 2021); and Austin, *National Defense Strategy*.

69. Nguyen, "Jus Ad Bellum," 1125.

70. Stockburger, "Known Unknowns," 31.

Defense and homeland security entities must coordinate efforts in order to understand the gravity of potential attacks and to respond appropriately. Providing mechanisms for timely analysis of an attack to clearly determine attribution is also needed. Additional research and clarification are necessary to work toward agreed-upon terms for cyberspace operations and gray-zone activities. Defining appropriate actions related to a response once attribution is determined will also clarify the course of action the government under attack should take. In addition to potential physical damage, defense entities should not underestimate the potential negative impact of significant gray-zone cyberattacks from digital, economic, and societal harm perspectives as the Department strives to deter those actions that threaten national security. Æ