A HOOVER INSTITUTION ESSAY

Cyberattack Attribution as Empowerment and Constraint

KRISTEN E. EICHENSEHR

Aegis Series Paper No. 2101

Introduction

When a state seeks to defend itself against a cyberattack, must it first identify the perpetrator responsible? The US policy of "defend forward" and "persistent engagement" in cyberspace raises the stakes of this attribution question as a matter of both international and domestic law.

International law addresses in part the question of when attribution is required. The international law on state responsibility permits a state that has suffered an internationally wrongful act to take countermeasures, but only against the state responsible. This limitation implies that attribution is a necessary prerequisite to countermeasures. But international law is silent about whether attribution is required for lesser responses, which may be more common. Moreover, even if states agree that attribution is required in order to take countermeasures, ongoing disagreements about whether certain actions, especially violations of sovereignty, count as internationally wrongful acts are likely to spark disputes about when states must attribute cyberattacks in order to respond lawfully.

Under domestic US law, attributing a cyberattack to a particular state bolsters the authority of the executive branch to take action. Congress has authorized the executive to respond to attacks from particular countries and nonstate actors in both recent cyber-specific statutory provisions and the long-standing Authorizations for Use of Military Force (AUMFs) related to 9/11 and the Iraq War. Attribution to one of these congressionally designated sources of attack ensures that the executive branch need not rely solely on the president's independent constitutional authority as commander in chief when responding, but instead can act with the combined authority of Congress and the president.[1]

Common across international and US law is the fact that cyberattack attribution serves as both a potential source of empowerment and a potential constraint on governmental action. In both systems, attribution of a cyberattack to another state bolsters the US executive branch's authority to respond, and conversely, the absence of attribution can place the executive on less certain legal footing.

This essay proceeds in three parts. It first explains cyberattack attribution and attribution's interaction with existing international law on the use of force and state responsibility.

The next section turns to the US "defend forward" policy and explores how it may spur disagreements about when states must attribute cyberattacks, even if they agree on the general legal framework set out in the first part. The essay then briefly addresses US domestic law and explains how congressional authorizations for certain military actions depend on attribution. The conclusion discusses how attribution can shape, not just be shaped by, the international and domestic legal systems.

Attribution and International Law

Cyberattack attribution is the process of assigning responsibility for the commission of a cyberattack.[2] Attribution has technical, legal, and policy aspects, and it can proceed at different levels. Cyberattack attributors might identify one or some combination of (1) the machine from which an attack was launched, (2) the individual who operated the machine, and (3) the organization or entity (if any) that directed the individual's actions.[3] As Herb Lin has noted, "although these three types of attribution are conceptually distinct, they are often related" because attributing an attack to a particular machine "may provide some clues that can help uncover the identity of the human perpetrator," which can in turn "help identify the party ultimately responsible for setting the entire intrusion into motion."[4]

In practice, the technical challenges of making attributions are significant, and attackers can make attributions more difficult by deliberately disguising their identities in so-called "false flag" operations.[5] Although the US government has signaled that its technical attribution capabilities have improved in recent years, tying a particular cyberattack to an individual and especially to a state raises legal and political issues, not just technical ones.[6]

International law on state responsibility uses the term *attribution* to "denote the operation of attaching a given action or omission to a State."[7] The international law on state responsibility sets out specific requirements for when actions are attributable to a state. Although not codified in a treaty, many provisions of the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts are understood to reflect customary international law.[8] Most basically, the articles specify that the conduct of "any State organ" is attributable to the state.[9] A state cannot, however, avoid international responsibility by outsourcing governmental functions. The "conduct of a person or entity which is not an organ of the State . . . but which is empowered by the law of that State to exercise elements of the governmental authority" is attributable to the state so long as "the person or entity is acting in that capacity in the particular instance."[10] Similarly, a state is responsible for the actions of persons or groups if they act "on the instructions of, or under the direction or control of, that State in carrying out . . . conduct."[11] The International Court of Justice has interpreted this standard to mean that a state is responsible if it exercises "effective control" over the actions of a nonstate actor.[12] "Effective control" means directing or controlling specific operations involving wrongful acts by a nonstate actor; providing

generalized support or direction is not sufficient to render a nonstate actor's wrongful actions attributable to a state.[13]

While the Draft Articles on State Responsibility provide detailed answers to when states *may* attribute conduct to other states and the relationships that suffice for such attribution, the articles and customary international law are less clear about the question on which this essay focuses, namely, when *must* states attribute cyberattacks to another state? International law answers this question only implicitly. In the current context, states must attribute internationally wrongful acts, including cyberattacks, if they want to take responsive action that would otherwise violate international law, including using force in self-defense or engaging in countermeasures.

Above the use-of-force threshold, the UN Charter recognizes states' customary international law right to engage in forcible self-defense in the face of an armed attack.[14] But in order for such use of force to be lawful, it must respond to an actual or imminent armed attack and be directed against the attacking entity.[15] Otherwise, the victim state's use of force would be offensive, not defensive, and thus prohibited by the UN Charter.[16]

The same logic underlies the requirement for a state to attribute an internationally wrongful act in order to take countermeasures. Countermeasures are actions that would be illegal under international law in general but are legally permissible for a state to take if it is responding to a prior unlawful act taken by another state.[17] The International Court of Justice has explained that a countermeasure "must be taken in response to a previous international wrongful act of another State and *must be directed against that State*."[18] Similarly, the ILC Draft Articles specify: "An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its [legal obligations]."[19] They further clarify that the "only" "is intended to convey that countermeasures may only be adopted against a State which is the author of the internationally wrongful act."[20]

In discussing countermeasures in response to cyberattacks, states have acknowledged the necessity of attributing a given cyberattack to a particular state. Then–State Department legal adviser Brian Egan noted in a 2016 speech that "the availability of countermeasures to address malicious cyber activity requires a prior internationally wrongful act that is attributable to another State."[21] UK attorney general Jeremy Wright made the link to attribution even clearer in explaining that "[a] countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state," which "means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response."[22]

The lawfulness of a countermeasure thus depends not only on attributing the cyberattack to another state, but also on doing so accurately. A countermeasure launched based on an

erroneous attribution turns the acting state from a victim into a perpetrator,[23] making its countermeasure not a countermeasure at all but an internationally wrongful act that could itself justify countermeasures.[24] The lawfulness of any countermeasure, then, depends on the accuracy of the attribution of the initial internationally wrongful act.

While states must attribute cyberattacks or other internationally wrongful acts in order lawfully to respond using countermeasures, states can also react in ways that do not require such attribution. For example, instead of countermeasures, a state that suffers an internationally wrongful act may instead choose not to respond at all or to engage only in retorsion—"'unfriendly' conduct which is not inconsistent with any international obligation of the State engaging in it."[25] Traditional examples of retorsion include severing diplomatic relations, declaring diplomatic personnel *persona non grata*, and imposing economic sanctions.[26] Some retorsion may be specific to the cybersecurity context. For example, the Netherlands has suggested that "a state may consider . . . limiting or cutting off the other state's access to servers or other digital infrastructure in its territory, provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory."[27] There is no extant international law requirement to engage in attribution as a predicate to retorsion.[28] States may engage in such unfriendly acts whenever and against whomever they please, so long as they comply with their treaty and customary international law obligations. Thus, a state engaging in retorsion need not identify a prior wrongdoing state in order to legally justify its own behavior. By definition, retorsion is always lawful.

Importantly, a legal requirement to attribute an internationally wrongful act in order to justify self-defense or countermeasures is not the same as a requirement to attribute *publicly*. States have reserved the right *not* to attribute publicly, even while recognizing a legal obligation to engage in attribution in particular circumstances.[29] They may instead communicate a cyberattack attribution to the perpetrator state privately, or quietly share the attribution with allies or other states.[30] Conversely, states may choose to attribute even lawful actions to other states, if they believe the behavior is malign. In other words, a public attribution does not mean that the attributed behavior is necessarily unlawful, nor does the absence of a public attribution mean that the victim state considers the behavior to be lawful.

However, even though public attribution is not presently legally required, there can be advantages to going public.[31] Prominent among them is avoiding confusion about the legal basis for a state's action. Consider a state that suffers a cyberattack that it understands to constitute an internationally wrongful act but that does not cause publicly observable effects. If the victim state engages in countermeasures that *are* publicly observable or otherwise discoverable, then unless it publicly attributes the initial wrongful act and explains that its actions are countermeasures, it risks having its own conduct misunderstood as an internationally wrongful act. Such misunderstandings may be

especially likely with respect to cyberattacks and cyber countermeasures because their effects are often less easily observable than are more conventional intrusions, and a cyber tit-for-tat exchange is less easily understood by outside observers than is a more tangible and traditional one.

Attribution in the Era of "Defend Forward"

Even if states agree that attribution is required before a victim state takes countermeasures, disagreements about what counts as an internationally wrongful act triggering a right to countermeasures raise the prospect of conflicts over when states must make attributions. The lack of clarity about what is lawful and unlawful is particularly acute below the use-of-force threshold, where the bounds of prohibited intervention are unclear,[32] and states openly disagree about the existence of a standalone rule barring violations of sovereignty. The US Department of Defense's "defend forward" policy puts significant pressure on these areas of disagreement and stakes out a US position setting a high bar for activity in cyberspace to be considered unlawful. It remains to be seen whether the US view will prevail, and in the meantime, states with a different view of the legal lines could well demand attribution in cases where the United States would argue attribution is not required. This section briefly explains the "defend forward" policy and then addresses how disagreements over the primary rules of state behavior below the use-of-force threshold interact with attribution. In short, where states disagree about whether a particular action violates international law, they will also disagree about whether countermeasures are available and thus about whether attribution is required.

The United States announced its "defend forward" policy in 2018 in a new Department of Defense (DoD) Cyber Strategy and a US Cyber Command (CYBERCOM) "Command Vision" document.[33] The strategy has both locational and temporal aspects. The DoD Cyber Strategy explains: "We will *defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict," and it states that "defend forward" requires "leveraging [the Defense Department's] focus outward to stop threats before they reach their targets."[34] CYBERCOM's Command Vision makes clear that DoD's policy is not purely defensive in the sense of taking defensive activity only on DoD or US networks. Rather, it focuses on taking actions "as close as possible to adversaries and their operations," wherever they may be.[35] Consistent with the goal of meeting adversaries where they are, the policy also encompasses a temporal component of persistent or continuous engagement.[36] The Command Vision explains:

> Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.[37]

Together, "defend forward" and "persistent engagement" make clear that the US strategy for cyberspace is to act consistently and around the world to disrupt hostile cyber activities aimed at the United States.

The "defend forward" policy's emphasis on actions outside of DoD and US networks runs headlong into an ongoing debate about whether international law prohibits violations of sovereignty that do not amount to a prohibited intervention or use of force. The debate is often framed as one between those who argue that sovereignty is a principle in international law that informs other rules,[38] and those who argue instead that sovereignty is a standalone rule, such that violations of sovereignty constitute an independent violation of international law even when they do not amount to intervention or use of force.[39] The influential *Tallinn Manual 2.0* controversially sided with the sovereignty-as-a-rule camp,[40] and states have increasingly lined up on one side of the debate or the other.

The United Kingdom has definitively taken the position that sovereignty is a principle, not a rule.[41] The US government also seems to lean in that direction. In a March 2020 speech at the US Cyber Command Legal Conference, DoD general counsel Paul Ney Jr. asserted: "For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."[42] He cited the example of espionage, which states prohibit in domestic law, but which "international law, in our view, does not prohibit . . . *per se* even when it involves some degree of physical or virtual intrusion into foreign territory."[43] If international law did treat sovereignty as a rule, it would be difficult to explain how at least some instances of espionage would not run afoul of a prohibition on violations of sovereignty.

An increasing number of states have taken the opposite position. In a 2019 white paper on the "International Law Applied to Operations in Cyberspace," France's Ministry of the Armies asserted that "any unauthorised penetration by a State of French systems or any production of effects on French territory . . . may constitute, at the least, a breach of sovereignty."[44] Similarly, the Netherlands has asserted that "respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act."[45] Austria, the Czech Republic, and Iran also appear to endorse the sovereignty-as-a-rule position,[46] and Finland and New Zealand recently joined the sovereignty-as-a-rule camp as well.[47] Even among states that endorse sovereignty-as-a-rule, however, the exact boundaries of what such a rule encompasses remain unclear.[48]

States' divergent views on the sovereignty question may cause disagreements over when states must attribute cyberattacks. Consider a hypothetical US operation to take down a

botnet.[49] Botnets are networks of malware-infected computers that can be used for a variety of purposes, such as distributed denial of service attacks and launching of ransomware. The hypothetical botnet—let's call it "Hypobot"—deploys ransomware against US small businesses, and the United States believes that Hypobot's operators are Russian-speaking cybercriminals, affiliated in some way with the Russian government. The United States could launch a counter-botnet operation that takes control of the botnet's command and control servers around the world and effectively severs communication to infected computers, disabling the botnet's operation.[50] From the US perspective, which seems to favor sovereignty-as-a-principle, neither the actions of the botnet operators against US businesses nor the US botnet takedown operation to access servers in countries around the world would violate international law. Neither action would constitute a use of force or prohibited intervention, and because sovereignty is a principle, not a rule, there is no internationally wrongful act and thus no need to invoke countermeasures or engage in attribution.

Consider the same operation, however, from the perspective of a state that endorses the sovereignty-as-a-rule view. Such a state would likely recognize the botnet's actions against US institutions as violations of US sovereignty—internationally wrongful acts—and thus conclude that the United States is entitled to take countermeasures *if the United States attributes the botnet's operations to the Russian government*. Countermeasures can only be taken against states, so a sovereignty-as-a-rule state's view of the lawfulness of the US operation would depend on whether or not the United States attributed the botnet to the Russian government.[51] If it did not, then the sovereignty-as-a-rule approach could categorize the US counter-botnet operation as itself perpetrating unlawful violations of sovereignty and entitling affected states to take countermeasures against the United States.[52]

Because only a few states have declared their position on the sovereignty question, considerable uncertainty remains about whether the silent majority of countries around the world that have yet to announce a view would regard the US actions as lawful or unlawful. Such uncertainty could cause friction or unintended escalation if, for example, the United States took actions to "defend forward" in or affecting a state that subscribed to (but had not announced) its adherence to the sovereignty-as-a-rule approach and then took countermeasures against the United States.[53]

DoD has made clear that it considers divergences in states' legal views in assessing available options for cyber actions. DoD general counsel Paul Ney Jr. noted in his March 2020 speech that in evaluating possible cyber operations, "even if a particular cyber operation does not constitute a use of force, it is important to keep in mind that the State or States targeted by the operation may disagree, or at least have a different perception of what the operation entailed."[54] With respect to countermeasures, Ney explained:

> In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a State within the timeframe in which the DoD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available.[55]

At first blush, this statement appears to be more definitive than Ney's statement about uses of force, going so far as to admit that countermeasures are not available if there is uncertainty or presumably disagreement about whether the triggering act is an international law violation.

But it raises the question: Who determines what counts as a countermeasure? Is a countermeasure defined by the sovereignty-as-a-rule camp or by the sovereignty-as-a-principle proponents? The United States would presumably argue that its cyber actions short of prohibited intervention or a use of force are simply retorsion, not internationally wrongful acts that would have to be justified as countermeasures. As noted above, retorsion does not require attribution to a state or compliance with the procedural and other limitations placed on countermeasures.[56] This leaves considerable room to "defend forward" against actions around the world that may not be attributed or attributable to states and to do so in ways that *other* states consider a violation of their sovereignty. This approach may well explain the recently reported Cyber Command operation to disrupt the TrickBot botnet—a ransomware botnet allegedly operated by Russian-speaking cybercriminals that has been used to disrupt health care providers and local governments, among others.[57] Although "what connection, if any, TrickBot's operators share with the Kremlin remains an open question," US officials were reportedly concerned that the botnet might be used to disrupt the 2020 election, on a state's orders or otherwise.[58] Consistent with the US view of sovereignty, the TrickBot takedown would not require attribution to a state and would not itself violate international law.

The other possible interpretation of Ney's statement about the unavailability of countermeasures is that the United States applies "defend forward" differentially depending on the state in which a cyber operation would occur or cause effects. For example, the United States may refrain from taking actions to counter cyber threats short of intervention or uses of force in states that endorse sovereignty-as-a-rule in instances where it cannot or does not wish to attribute the threat to a state actor. One problem with this approach, however, is that it would incentivize gamesmanship. If sovereignty-as-a-principle states were to defer to sovereignty-as-a-rule states' view about when attribution is required, states would have an incentive to declare their support for sovereignty-as-a-rule opportunistically in order to deter operations in their territory. It seems more likely that the United States follows its own sovereignty-as-a-principle view of what counts as an internationally wrongful act and thus when attribution is required, though doing so may well put it in a position of "defending forward" in ways that other states would consider internationally wrongful.

The Domestic Law Overlay

Although the implications of attribution are more significant with respect to international law, the executive branch's ability and willingness to attribute cyberattacks to particular states affects its domestic legal authorities as well. As part of the Article II Commander-in-Chief powers, the president has consistently claimed authority to deploy US armed forces without congressional authorization in situations short of war.[59] This extends to cyber-based actions as well as conventional ones.[60] Executive authority is understood to be "at its maximum," however, "when the President acts pursuant to an express or implied authorization of Congress."[61] Congress has passed several statutes authorizing executive actions in cyberspace, impliedly and expressly, but all depend on attribution.[62]

Congress expressly authorized cyber operations in the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[63] Section 1642 specifies that if "the National Command Authority determines that" Russia, China, North Korea, or Iran "is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes," then the National Command Authority may authorize Cyber Command "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks."[64] As stated, this authority depends on attribution of cyber operations to a particular set of states. If the executive does attribute cyber intrusions to Russia, China, North Korea, or Iran, then it need not act based solely on the president's constitutional powers, but rather can proceed with the combined constitutional authority of the executive and Congress.[65]

The executive can also invoke congressional authorization for cyber operations if they fall within existing general AUMFs. In particular, the 2001 AUMF, passed in the wake of the 9/11 attacks, authorizes the president "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons."[66] The 2002 Iraq AUMF authorizes the president "to use the Armed Forces of the United States as he determines to be necessary and appropriate in order to . . . defend the national security of the United States against the continuing threat posed by Iraq."[67] The broad authorizations in the AUMFs logically include force exercised via cyber means, but the extra authority they provide once again depends on attribution of attacks (whether cyber or otherwise) to those involved with the 9/11 attacks or to Iraq.[68]

Given the executive's capacious understanding of its constitutional authority to use force independent of congressional authorization,[69] the cyber-specific and more general authorizations for cyberattacks against particular perpetrator states may not materially change the executive's behavior. The 2019 NDAA cyber provision may simply "[function] as a belt-and-suspenders provision, mooting separation-of-powers objections that might

otherwise arise."[70] Nonetheless, it is notable that when Congress specifically considered and passed legislation to empower Cyber Command, it chose to make the authorization dependent on attribution to particular states, rather than generally authorizing Cyber Command to respond in "foreign cyberspace" to *any* "active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace" by state or nonstate actors.[71]

The 2019 NDAA is likely not Congress's last word on the subject of cyberattack attributions. As part of a report on cyberspace policy required by the 2019 NDAA, Congress specified that the president must provide "information relating to the Administration's plans, including specific planned actions, regulations, and legislative action required, for . . . advancing technologies in attribution."[72] Similarly, the Senate Select Committee on Intelligence Report on Russian election interference, released in July 2019, argues that the government "should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy" and that "timely and accurate attribution is not only important to defensive information sharing, but will also underpin a credible deterrence and response strategy."[73] Both Congress's enactments and international law ensure that attribution is indeed key to responding to cyberattacks.

Conclusion

Attributing a cyberattack to a state can empower the victim state by allowing it to take lawful countermeasures, and in US domestic law, attributions of particular kinds of attacks to specific states bolster the legal authority for executive action. But the requirement to attribute also functions as a constraint: victim states cannot engage in countermeasures unless they make an attribution to a state, and in the US system, the executive cannot rely on congressional authorization unless it attributes to a particular set of states.

This legal analysis, however, is not the end of the story on attributions. Public attributions of cyberattacks can play a role beyond justifying responsive actions. They can help to shape, not just be controlled by, international and domestic US law. Public attributions of cyberattacks to governments bring to light the often murky world of state practice in cyberspace, and by declaring certain behaviors to be unacceptable, they can help to shape the rules of the road for state behavior going forward.[74] Attributions, especially if coordinated among groups of countries and accompanied by real consequences such as economic sanctions, can play a constitutive role, solidifying and enforcing norms of responsible behavior in cyberspace that might eventually crystallize into customary international law. Attributions can also shape domestic US authorities by revealing which states are operating against the United States in cyberspace and perhaps prompting Congress to authorize additional operations in cyberspace.

ACKNOWLEDGMENTS

Thanks to Gary Corn, Ashley Deeks, Jack Goldsmith, and Richard Re for helpful comments and conversations, and to Hannah Keefer for excellent research assistance.

NOTES

1 *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) (describing Category 1 in which "the President acts pursuant to an express or implied authorization of Congress," and therefore "his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate"); *see also infra* section 3 "The Domestic Law Overlay."

2 Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, 522 (2020).

3 *See*, *e.g.*, Herbert Lin, *Attribution of Malicious Cyber Incidents* 5 (Hoover Inst. Working Group on Nat'l Sec., Tech., and L., Aegis Series Paper No. 1607, 2016), https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf (explaining that the question of "who is responsible" for a cyberattack "can be answered in three ways . . . a machine, a specific human being pressing the keys or otherwise setting the intrusion into motion, and an ultimately responsible party").

4 *Id*. at 13.

5 For discussions of the technical side of attribution, including types of evidence that can lead to identification of individual and state perpetrators, see *id*. at 5–11; Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. Strat. Stud. 4, 14–23 (2015). For discussion of Russian false flag operations, see, for example, Andy Greenberg, *A Brief History of Russian Hackers' Evolving False Flags*, Wired (Oct. 21, 2019), https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/, and Michael S. Schmidt & Nicole Perlroth, *U.S. Charges Russian Intelligence Officers in Major Cyberattacks*, N.Y. Times (Oct. 19, 2020), https://www.nytimes.com/2020/10/19/us/politics/russian-intelligence-cyberattacks.html.

6 *See*, *e.g.*, Eichensehr, *supra* note 2, at 531 (detailing US government statements about improvements in its attribution capabilities).

7 Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, UN Doc. A/56/10, at 36 (2001).

8 *See*, *e.g.*, Ashley Deeks, *Defend Forward and Cyber Countermeasures* 2 (Hoover Inst. Working Group on Nat'l Sec., Tech., and L., Aegis Series Paper No. 2004, 2020), https://www.hoover.org/research/defend-forward-and-cyber-countermeasures (noting that "many states view the [Draft Articles] as reflecting customary international law"). Although the United States has taken issue with some provisions, *see infra* note 56, the State Department's understanding of international law appears to track the Draft Articles on the basic rules for attributing actions to states and states' entitlement to take countermeasures, *see*, *e.g.*, U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (Oct. 2014), *in* Digest of U.S. Practice in International Law 732, 738–39 (2014), https://2009-2017.state.gov/documents/organization/244504.pdf.

9 Int'l L. Comm'n, *supra* note 7, at 40.

10 *Id*. at 42; *see also id*. at 42–43 (discussing examples of entities that fall within Article 5). A state remains responsible for the actions of state organs and entities empowered to exercise governmental functions even if "the organ, person, or entity . . . exceeds its authority or contravenes instructions." *Id*. at 45. A state also incurs international responsibility for the conduct of organs of another state that are placed at its disposal and exercising governmental authority on its behalf. *Id*. at 43–44.

11 *Id*. at 47.

12 Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 115 (June 27) (explaining that for conduct of a nonstate armed group to be attributed to a state "it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed").

13 Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. and Herz. v. Serb. and Montenegro), 2007 I.C.J. Rep. 43, ¶ 400 (Feb. 26) (clarifying that in order for state responsibility to attach, a state must exercise "effective control" or give instructions "in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations"). *But see* Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶ 145 (Int'l Crim. Trib. for the Former Yugoslavia, July 15, 1999), https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf (adopting a lower standard of "overall control" for state responsibility for the actions of nonstate armed groups).

14 UN Charter Art. 51.

15 *See*, *e.g.*, Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the Int'l Legal Order in Cyberspace, Appendix at 8–9 (July 5, 2019) (Neth.) [hereinafter Netherlands Letter], https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf ("The burden of proof for justifiable self-defence against an armed attack is a heavy one. . . . States may . . . use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain.").

16 UN Charter Art. 2(4).

17 Int'l L. Comm'n, *supra* note 7, at 128 (defining countermeasures as "measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation").

18 Case Concerning the Gabčíkovo–Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7, ¶ 83 (Sept. 25) (emphasis added).

19 Int'l L. Comm'n, *supra* note 7, at 129.

20 *Id*. at 130. For avoidance of all doubt, the Articles further explain: "Countermeasures may not be directed against States other than the responsible State." *Id*.

21 Brian J. Egan, *International Law and Stability in Cyberspace*, 35 Berkeley J. Int'l L. 169, 178 (2017).

22 Attorney General Jeremy Wright QC MP, United Kingdom, Address at Chatham House Royal Institute for International Affairs: Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; *see also* Netherlands Letter, *supra* note 15, at 6 ("For a state to be held responsible under international law for a cyber operation and, by extension, for a target state to be able to take a countermeasure in response, it must be possible to attribute the operation to the state in question." [footnote omitted]).

23 Int'l L. Comm'n, *supra* note 7, at 130 ("A State taking countermeasures acts at its peril, if its view of the question of wrongfulness turns out not to be well founded . . . and [it] may incur responsibility for its own wrongful conduct in the event of an incorrect assessment."); *see also* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 82–83 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0] (explaining that "States taking countermeasures based on a decision that another State has breached an obligation owed to them do so at their own risk," and "Thus, while it might be reasonable to take a

countermeasure . . . , for instance because significant evidence exists to support attribution to a State against which the cyber countermeasure is taken, if the conclusion as to attribution proves to be flawed, . . . the State itself will have committed an internationally wrongful act").

24 *See* Egan, *supra* note 21, at 178 (explaining that a state attempting to engage in countermeasures may be "held responsible for violating international law if it turns out that there wasn't actually an internationally wrongful act that triggered the right to take countermeasures, or if the responding State made an inaccurate attribution determination" and therefore that "countermeasures should not be engaged in lightly"); *see also* Deeks, *supra* note 8, at 6 (explaining that "States taking countermeasures in response to wrongful cyber activity bear the burden of attributing the wrongful activity to which they are responding to the proper actors—just as they do when responding to wrongful activity outside of cyberspace," and noting that "the elevated risk of misattribution in the cyber context suggests that states should have high levels of confidence before taking countermeasures in response to malicious cyber operations").

25 Int'l L. Comm'n, *supra* note 7, at 128; *see also* Egan, *supra* note 21, at 177 ("A State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States.").

26 *See*, *e.g.*, Int'l L. Comm'n, *supra* note 7, at 128 ("Acts of retorsion may include the prohibition of or limitations upon normal diplomatic relations or other contacts, embargoes of various kinds or withdrawal of voluntary aid programmes."); Egan, *supra* note 21, at 177 (citing examples of retorsion including "the imposition of sanctions or the declaration that a diplomat is *persona non grata*").

27 Netherlands Letter, *supra* note 15, at 7; *see also* Tallinn Manual 2.0, *supra* note 23, at 112 (Rule 20) cmt. 4 (suggesting that, as a type of retorsion, "a State may . . . employ an access control list to prevent communications from another State . . . so long as it violates no treaty obligation or applicable customary law norm").

28 In a forthcoming article, Martha Finnemore & Duncan Hollis argue: "For a state to engage in either retorsion or counter-measures, however, requires some accusation articulating the requisite wrongful acts that form the basis for it to pursue the enforcement of its legal rights." Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, Eur. J. Int'l L. (forthcoming 2020) (manuscript at 12), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347958. It is not clear whether they mean to argue that states are required to engage in cyberattack attribution before engaging in retorsion, because elsewhere in the same paper they argue that what they term "accusations" "can occur without attribution (i.e., when accusers say, 'we do not know who did this, but it happened, and it was bad')." *Id*. (manuscript at 8).

29 *See, e.g.*, Wright, *supra* note 22 (recognizing that a state engaging in countermeasures "must be confident in its attribution of that act to a hostile state before it takes action in response" but also explaining that "there is no legal obligation requiring a state . . . to publicly attribute hostile cyber activity that it has suffered in all circumstances" and that the United Kingdom sometimes attributes "publicly" and "sometimes . . . do[es] so only to the country concerned").

30 See French Ministry of the Armies, International Law Applied to Operations in Cyberspace 10 (2019), https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (stating that "the identification of a State as being responsible for a cyberattack that is an internationally unlawful act does not in any way oblige the victim State to make a public attribution," and that "France reserves the right to attribute publicly, or not, a cyberattack against it and to bring that information to the attention of its population, other States or the international community"); *see also* Greg Miller et al., *Obama's Secret Struggle to Punish Russia for Putin's Election Assault*, Wash. Post (June 23, 2017), https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/ (reporting that President Obama privately warned Vladimir Putin in September 2016 to stop Russia's efforts to interfere in the election and that the first US public attribution to Russia occurred in October 2016).

31 I have elsewhere argued that recent public attributions bring transparency to state practice in cyberspace and can have an important influence on setting norms and customary international law to govern state behavior. *See* Eichensehr, *supra* note 2, at 556–58.

32 *See, e.g.*, Gary P. Corn, *Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention* 6–14 (Hoover Inst. Working Group on Nat'l Sec., Tech., and L., Aegis Series Paper No. 2005, 2020), https://www.hoover.org/sites/default/files/research/docs/corn_webready.pdf (discussing uncertainty and disagreements about the boundaries of the nonintervention rule, especially in the cybersecurity context).

33 *See* US Dep't of Def., Summary: Department of Defense Cyber Strategy (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; US Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

34 US Dep't of Def., *supra* note 33, at 1; and at 2.

35 US Cyber Command, *supra* note 33, at 6.

36 For an explanation of the relationship between "defend forward" and "persistent engagement," see Hon. Paul C. Ney Jr., General Counsel, Dep't of Def., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (March 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; *see also The Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace: Hearing Before the H. Comm. on Armed Servs., Subcomm. on Intelligence and Emerging Threats and Capabilities*, 116th Cong. 44 (2020) (written statement of Gen. Paul M. Nakasone, commander, US Cyber Command) (describing "defend forward" as the "strategic direction" that "drives Cyber Command's doctrine called persistent engagement").

37 US Cyber Command, *supra* note 33, at 6.

38 *See, e.g.*, Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 Am. J. Int'l L. Unbound 208 (2017) (arguing that below the thresholds of use of force or intervention, "there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law").

39 *See, e.g.*, Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace:* Lex Lata Vel Non*?*, 111 Am. J. Int'l L. Unbound 213 (2017) (defending the *Tallinn Manual* position that sovereignty is an independent rule of international law).

40 Tallinn Manual 2.0, *supra* note 23, at 17–27 (Rule 4).

41 Wright, *supra* note 22 (noting that although "some . . . argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent," he was "not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention," and explaining that "[t]he UK Government's position is therefore that there is no such rule as a matter of current international law").

42 Ney, *supra* note 36.

43 *Id*.

44 French Ministry of the Armies, *supra* note 30, at 6. The extent to which this view represents the position of the entire French government as opposed to only the Ministry of the Armies is unclear. *See* Col. Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, Just Sec. (Feb. 11, 2020), https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/ (noting that "the French document does not claim to be the official position of the French

government," but rather may be more akin to the "DoD Law of War Manual which does not necessarily reflect the views of the U.S. Government as a whole").

45 Netherlands Letter, *supra* note 15, at 2.

46 *See* Przemysław Roguski, *The Importance of New Statements on Sovereignty in Cyberspace by Austria*, *the Czech Republic and United States*, Just Sec. (May 11, 2020), https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/ (noting that in conjunction with the UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, Austria and the Czech Republic have both endorsed the sovereignty-as-a-rule position); Przemysław Roguski, *Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace*, Just Sec. (Sept. 3, 2020), https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/ (providing an overview of the statement on international law issued by the General Staff of the Iranian Armed Forces, including Iran's apparent endorsement of the sovereignty-as-a-rule position, but also noting caveats about the extent to which the statement itself and especially the available English translation reflect official Iranian policy).

47 Finnish Gov't, Min. for For. Aff., Press Release, Finland Published Its Positions on Public International Law in Cyberspace (Oct. 15, 2020), https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace ("Finland sees sovereignty as a primary norm of public international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility."); New Zealand For. Aff. & Trade, The Application of International Law to State Activity in Cyberspace (Dec. 1, 2020), https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/ ("New Zealand considers that the standalone rule of territorial sovereignty also applies in the cyber context but acknowledges that further state practice is required for the precise boundaries of its application to crystallise.").

48 *See*, *e.g.*, Netherlands Letter, *supra* note 15, at 2–3 (endorsing the sovereignty-as-a-rule position, while also noting that the "precise boundaries of what is and is not permissible have yet to fully crystallise"). For example, states that endorse the sovereignty-as-a-rule position might nonetheless include an exception for de minimis intrusions on sovereignty. *Cf.* Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, Director of Cybersecurity Department, 2nd Substantive Session of the Open-Ended Working Group on Developments in the Field of Info. & Telecomm. in the Context of Int'l Sec. of the First Comm. of the General Assembly of the United Nations Feb. 11, 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf (explaining that "[t]he Czech Republic concurs with those considering the principle of sovereignty as an independent right," but listing examples of violations of sovereignty that appear to exclude those below certain thresholds); New Zealand For. Affs. & Trade, *supra* note 47 (explaining New Zealand's view that although "sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state," there remains "a range of circumstances—in addition to pure espionage activity—in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful").

49 Such operations are not hypothetical, though the details of the in-text hypothetical are. *See* Ellen Nakashima, *Cyber Command Has Sought to Disrupt the World's Largest Botnet*, *Hoping to Reduce Its Potential Impact on the Election*, Wash. Post (Oct. 9, 2020), https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html (reporting that Cyber Command disrupted the TrickBot botnet, which was "run by Russian-speaking criminals" and for ransomware); David E. Sanger & Nicole Perlroth, *Microsoft Takes Down a Risk to the Election*, *and Finds the U.S. Doing the Same*, N.Y. Times (Oct. 12, 2020), https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html (reporting on Microsoft and Cyber Command's operations to take down the TrickBot botnet).

50 For examples of the mechanics used in takedowns, see, for example, Robert Chesney, *Persistently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet*, Lawfare (Oct. 12, 2020), https://www.lawfareblog.com

/persistently-engaging-trickbot-uscybercom-takes-notorious-botnet; Brian Krebs, *U.S. Government Takes Down Coreflood Botnet*, Krebs on Security (Apr. 11, 2011), https://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet/.

51 *See* Int'l L. Comm'n, *supra* note 7, at 129 ("An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act."); *see also* Tallinn Manual 2.0, *supra* note 23, at 113 (Rule 20) cmt. 7 ("Countermeasures are not available in response to a cyber operation conducted by a non-State actor unless the operation is attributable to a State."); Col. Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, Just Sec. (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ (arguing that the sovereignty-as-a-rule approach is problematic in part because "unlike self-defense, countermeasures cannot be invoked as a justification for actions taken against non-state actors" and thus a state seeking to take down a botnet operated by a nonstate actor "can do so only with the consent of each State in whose territory the cyber action will occur, or based on a reasonable determination that those States are themselves in breach of an international obligation").

52 The analysis becomes even more complicated if the botnet command-and-control servers are located in third states. Although countermeasures may "incidentally affect the position of third States," if "a third State is owed an international obligation by the State taking countermeasures and that obligation is breached by the countermeasure, the wrongfulness of the measure is not precluded as against the third State." Int'l L. Comm'n, *supra* note 7, at 130. In other words, if the United States were to act against a command-and-control server in, for example, France, then at least according to the sovereignty-as-a-rule position, the United States could thereby breach a legal duty not to violate France's sovereignty. The US action might *not* constitute an unlawful violation of France's sovereignty if there is a de minimis exception to violations of sovereignty, *see supra* note 48, or if France had breached a duty of due diligence, which would itself violate international law and entitle the United States to take countermeasures. *See*, *e.g.*, Tallinn Manual 2.0, *supra* note 23, at 30–50 (Rule 6) (discussing due diligence).

53 *Cf.* Egan, *supra* note 21, at 172 (recognizing that "states' relative silence could lead to unpredictability in the cyber realm, where States may be left guessing about each other's views on the applicable legal framework," and therefore that "in the context of a specific cyber incident, this uncertainty could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict").

54 Ney, *supra* note 36. He made a very similar point about nonintervention, explaining that "[b]ecause States take different views on this question [of the scope of the prohibition on intervention], DoD lawyers examining any proposed cyber operations must tread carefully, even if only a few States have taken the position publicly that the proposed activities would amount to a prohibited intervention." *Id*.

55 *Id*.

56 The ILC Draft Articles on State Responsibility set out a variety of procedural limitations on how countermeasures may be deployed, including that the injured state must call on the offending state to cease the internationally wrongful act and offer to negotiate before engaging in countermeasures. *See* Int'l L. Comm'n, *supra* note 7, at 134–37. Some states have challenged such provisions as not reflective of customary international law. *See*, *e.g.*, Ney, *supra* note 36 (noting "varying State views on whether notice would be necessary in all cases [of countermeasures] in the cyber context because of secrecy or urgency"); Wright, *supra* note 22 ("[W]here the UK is responding to covert cyber intrusion with countermeasures[,] . . . we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it."); *see also* Sean D. Murphy, *U.S. Comments on ILC Draft Articles on State Responsibility*, 95 Am. J. Int'l L. 626, 626–28 (2001) (reporting US government comments on the ILC Draft Articles that characterized provisions on countermeasures as not reflective of customary international law).

57 Nakashima, *supra* note 49; *see also* Chesney, *supra* note 50 (discussing the TrickBot operation as an example of persistent engagement).

58 Sanger & Perlroth, *supra* note 49.

59 For details on the executive's argument for presidential authority to use force, see, for example, Memorandum Opinion from Karl R. Thompson, Principal Deputy Assistant Att'y Gen., Office of Legal Couns., to the Couns. to the President, Authority to Order Targeted Airstrikes Against the Islamic State of Iraq and the Levant (Dec. 30, 2014); Memorandum Opinion from Caroline D. Krass, Principal Deputy Assistant Att'y Gen., Office of Legal Couns., to the Att'y Gen., Authority to Use Military Force in Libya (Apr. 1, 2011).

60 *See* Ney, *supra* note 36 ("The domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation."); *see also* Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations* 5 (Hoover Inst. Working Group on Nat'l Sec., Tech., and L., Aegis Series Paper No. 2003, 2020), https://www.hoover.org/research/domestic-legal-framework-us-military-cyber-operations (discussing the Office of Legal Counsel's high bar for when congressional authorization is required for military operations and suggesting that most cyber operations would not reach the level of "war" that the Office of Legal Counsel (OLC) believes is the triggering requirement for congressional authorization).

61 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring).

62 *See* Chesney, *supra* note 60, at 3–5 (discussing the AUMFs and Section 1642 of the 2019 NDAA as statutory authorizations available to US Cyber Command).

63 Pub. L. No. 115-232, 132 Stat. 1636 (codified at 10 U.S.C. § 394 note (2018)).

64 *Id*. § 1642(a)(1), 132 Stat. at 2132.

65 *See* Ney, *supra* note 36 (arguing that "in the context of cyber operations, the President does not need to rely solely on his Article II powers because Congress has provided for ample authorization," including in the 2019 NDAA and the 2001 AUMF).

66 Authorization for Use of Military Force, § 2(a), Pub. L. No. 107-40, 115 Stat. 224 (codified at 50 U.S.C. § 1541 note [2001]).

67 Authorization for Use of Military Force Against Iraq Resolution of 2002, § 3(a), Pub. L. No. 107-243, 116 Stat. 1498 (codified at 50 U.S.C. § 1541 note [2002]).

68 *See*, *e.g.*, Ney, *supra* note 36 ("Cyber operations against specific targets are logically encompassed within broad statutory authorizations to the President to use force, like the 2001 Authorization for Use of Military Force."). The Trump administration stretched the bounds of the 2002 AUMF beyond recognition when it argued that it authorized a drone strike on Iranian military commander Qassim Soleimani in Iraq in January 2020. *See generally* Jean Galbraith, *U.S. Drone Strike in Iraq Kills Iranian Military Leader Qasem Soleimani*, 114 Am. J. Int'l L. 313, 319 (2020) (citing a White House notice to Congress explaining that the president had authority for the strike under both his Article II Commander-in-Chief powers and the 2002 AUMF). Indeed, Congress itself rejected the administration's interpretation of the 2002 AUMF in a joint resolution, which President Trump subsequently vetoed. S. J. Res. 68, sec. 1(3), 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-joint-resolution/68/text. For additional criticism of the administration's interpretation, see Ryan Goodman, *White House '1264 Notice' and Novel Legal Claims for Military Action Against Iran*, Just Sec. (Feb. 14, 2020), https://www.justsecurity.org/68594/white-house-1264-notice-and-novel-legal-claims-for-military-action-against-iran/; Ryan Goodman & Steve Vladeck, *Why the 2002 AUMF Does Not Apply to Iran*, Just Sec. (Jan. 9, 2020), https://www.justsecurity.org/67993/why-the-2002-aumf-does-not-apply-to-iran/.

69 *See supra* note 59 and accompanying text (discussing OLC opinions on executive authority to conduct military operations).

70 Chesney, *supra* note 60, at 4–5.

71 Pub. L. No. 115-232, § 1642(a)(1), 132 Stat. at 2132.

72 *Id*. § 1636, 132 Stat. at 2127.

73 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 1, at 55 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

74 *See* Eichensehr, *supra* note 2, at 556–58; Finnemore & Hollis, *supra* note 28, at 14–17.

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Kristen E. Eichensehr, *Cyberattack Attribution as Empowerment and Constraint*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2101 (January 15, 2021), available at https://www.lawfareblog.com/cyberattack-attribution-empowerment-and-constraint.

About the Author

KRISTEN E. EICHENSEHR

Kristen E. Eichensehr is the Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor at the University of Virginia School of Law. She is a member of the editorial board of *Just Security* and an affiliate at the Stanford Center for International Security and Cooperation.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION