I. INTRODUCTION

Espionage, so the cliché goes, is the world’s second-oldest profession.\(^1\) Notwithstanding some debate in the academy about the legality of peacetime espionage under international law;\(^2\) and despite the tempering influence of occasional outcries for its cessation,\(^3\) espionage is a practice that states have long engaged in and acknowledged as a matter of practical reality.\(^4\) Enter cyber networks.\(^5\) The rise of the Internet and technological advances in computer and telecommunications networking have facilitated an information revolution begetting a multiplicity of benefits for innovation and economic growth. But the same technology that has

---


\(^4\) This acceptance stems from, inter alia, the lack of clarity in international law vis-à-vis intelligence activities and the consistent historical practices of states. See Chesterman, supra note 3, at 1072 (“Most domestic legal systems . . . seek to prohibit intelligence gathering by foreign agents while protecting the state’s own capacity to conduct such activities abroad.”); see also Christopher D. Baker, Tolerance of International Espionage: A Functional Approach, 19 AM. U. INT’L L. REV. 1091, 1092 (2004) (“[I]nternational law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation.”).

\(^5\) For purposes of this paper, the terms cyber, cyber network, and cyberspace refer to the “global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.” Daniel T. Kuehl, From Cyberspace to Cyberpower: Defining the Problem, in CYBERPOWER AND NATIONAL SECURITY 24, 28 (Franklin D. Kramer et al. eds., 2009).
yielded this cascade of “generativity” makes states vulnerable to acts of espionage and information warfare that threaten their economic and national security.\textsuperscript{6}

This development raises a host of questions about the evolving nature of espionage and its treatment under domestic and international legal regimes. In particular, three aspects of cyber security bring thorny legal issues to the fore: the ability of spies and hackers to access protected information from remote locations; problems of identity attribution with respect to perpetrators; and the difficulty of distinguishing acts of exploitation and theft from attacks and uses of force.

This paper focuses primarily on the third of these features and its consequences for the treatment of cyber intrusions under U.S. and international law. I will argue that the difficulty of distinguishing between cyber espionage and cyber attack entails a blurring of the conceptual and legal distinction between intelligence collection and covert action. In light of this practical reality, it would seem prudent to increasingly treat future network-based intrusions as covert actions rather than traditional intelligence collection—\textit{i.e.}, as attempts to influence conditions abroad, rather than as acts of espionage. This evolution in the practice and oversight of espionage would represent an acknowledgment of the inherent uncertainty attendant to the use of cyberspace as a medium for intrusion and the need for a credible deterrent structure absent the availability of traditional legal remedies for managing the threat (and offensive asset) posed by cyber networks.

This paper proceeds as follows. Part II defines key terms and surveys the domestic and international laws governing peacetime espionage and covert action. Part III explains three features of network-based espionage that distinguish it from traditional espionage, focusing on

the specific difficulty of distinguishing cyber exploitation from cyber attack. Part IV identifies how the exploitation/attack quandary renders much of the existing legal treatment of espionage inapt or inadequate. In doing so, it suggests a possible approach for the United States that would fit cyber intrusions within existing legal structures relating to covert action, a more appropriate framework of law and oversight for conceptualizing, initiating, and responding to acts of exploitation and attack in the cyber domain. Employing the covert action model would allow the government to establish a credible deterrent and retributive defense to cyber attack and exploitation whilst minimizing the risk that its own utilization of cyberspace oversteps the bounds of legality or generates negative consequences for national and international security. Part V concludes.

II. THE LAW OF ESPIONAGE AND COVERT ACTION

A complex web of law purports to regulate the offensive conduct of espionage and covert action while criminalizing these activities from a defensive standpoint. Domestic statutes governing U.S. intelligence collection and covert action find their roots in the National Security Act of 1947 and Executive Order 12333. Provisions criminalizing espionage against the United States are scattered throughout portions of Title 18, though defensive responses to covert action—insofar as they involve the projection of power abroad rather than through domestic criminal proceedings—are generally governed by international law. For its part, international law touches upon espionage only indirectly. While the status of covert actions under transnational legal regimes is a subject of some debate, there are no treaties or customary norms that explicitly proscribe the practice. Notwithstanding and perhaps in accord with this murkiness, international law plainly leaves room for states to exercise sovereignty both within
and beyond their territorial jurisdiction in crafting legal prohibitions on espionage and covert action.

A. Definition of Terms

As a threshold matter, it is important to clarify precisely what is meant by invocation of the term “espionage”, for it represents but one species of intelligence activity.7 Black’s Law Dictionary defines espionage as “[t]he practice of using spies to collect information about what another government or company is doing or plans to do.”8 In line with this definition, for purposes of this paper the terms espionage and “intelligence collection” will be used interchangeably and in contradistinction to “covert action”.9 With this definition as a starting point, it will be helpful to consider the legal architecture of espionage from both offensive and defensive perspectives. With respect to the former, this paper will survey laws regulating the actions of U.S. intelligence officers; regarding the latter, it will address the legal framework governing acts of espionage against the United States. Importantly, this discussion will be limited to analysis of intelligence collection during times of peace rather than in armed conflict, during which espionage is generally governed under the law of armed conflict (LOAC) paradigm.10

---

8 BLACK’S LAW DICTIONARY (8th ed. 2004), espionage.
9 The distinction between espionage and covert action is perhaps less clear in the literature than the distinction between intelligence collection and covert action. Cf. Radsan, supra note 7, at 599 (“Covert action . . . does not fit into the traditional categories of collection and analysis at intelligence agencies.”). However, much writing on the subject finds it useful to exclude covert action from discussions of “intelligence”. See, e.g., id. at 601 (defining intelligence narrowly to exclude covert action). Moreover, the simple fact that legal and standard dictionaries generally define “espionage” as a practice of information collection warrants the working definition set forth here. See, e.g., MERRIAM-WEBSTER’S ONLINE DICTIONARY (2010), espionage, available at http://www.merriam-webster.com/dictionary/espionage (defining espionage as “the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company”).
10 The Hague Regulations and the Geneva Convention Relative to the Protection of Civilian Persons in Time of War require “humane” treatment of spies captured during wartime and provide limited trial rights for such captives. See Chesterman, supra note 3, at 1079–80. The First Additional Protocol to the Geneva Conventions restates the customary norm that ruses of war are permitted but spies are not entitled to POW status unless they return to their
This working definition of espionage omits two categories of intelligence activity entrusted to the Intelligence Community (IC)\textsuperscript{11} by U.S. law: intelligence analysis and covert action.\textsuperscript{12} Analysis involves making sense of the various pieces of information procured from human and technical sources around the world.\textsuperscript{13} Covert action is defined in statute as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.”\textsuperscript{14} For purposes of this paper, the terms “espionage” and “collection” will be used interchangeably and will exclude both analysis and covert action. While intelligence analysis may be a practice rife with legal uncertainty,\textsuperscript{15} such questions are not within the scope of this discussion. As we shall see, however, the utilization of cyber networks in carrying out collection activities likely entails a measure of conceptual overlap with covert action. For this reason, the following overview surveys the treatment of both espionage and covert action under U.S. and international law.

B. United States Domestic Law

Federal statutes regulate the scope of U.S. government-directed espionage and covert action against foreign states while criminalizing espionage by foreign state actors. The following

\textsuperscript{11}“The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities.” Intelligence.gov, About the Intelligence Community, http://www.intelligence.gov/about-the-intelligence-community/ (last visited May 11, 2010).

\textsuperscript{12}See Radsan, \textit{supra} note 7.


\textsuperscript{15}See, e.g., Simon Chesterman, \textit{The Spy Who Came in from the Cold War: Intelligence And International Law}, 27 MICH. J. INT’L L. 1071, 1073 (2006) (“Some classified information might also be protected as intellectual property under the World Trade Organization-brokered Agreement on Trade-Related Aspects of Intellectual Property Rights. It might also conceivably be protected by the right to privacy enshrined in some human rights treaties. By contrast, intelligence analysis that relies on open source information is legally unproblematic.”).
discussion considers these offensive- and defensive-oriented laws regarding collection and covert action in turn.

1. Offensive Regulation

   i. Espionage

Authority for the conduct of foreign intelligence collection by the United States government is grounded in the “firm foundation” of the Constitution, the National Security Act of 1947 (NSAct), and the Central Intelligence Agency Act of 1949, as well as the many congressional appropriations for intelligence activities. Authority for Congress’s passage of statutes governing U.S. intelligence collection is drawn from its constitutional power to “provide for the common defense and general welfare of the United States.” Through the NSAct, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and other statutes, Congress conveys broad authority to the Central Intelligence Agency (CIA) to “collect intelligence through human sources [HUMINT] and by other appropriate means.” The Act also provides for, among other programs and agencies, the establishment of a signals intelligence (SIGINT) program to be coordinated by the Secretary of Defense through the National Security Agency (NSA), as an element of the National Intelligence Program overseen by the Director of National Intelligence (DNI). This set of provisions clearly authorizes the Intelligence Community to engage in clandestine foreign intelligence collection.

The DNI and heads of IC agencies are obligated by statute to keep the House and Senate intelligence committees “fully and currently informed” of all intelligence activities that are not

---

17 Radsan, supra note 7, at 601.
18 U.S. CONST. art I § 8, cl. 2.
22 See Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee), Foreign and Military Intelligence, S. REP. 94-755, Book I, at 128–31 (1976).
covert actions, “including any significant anticipated intelligence activity and any significant intelligence failure.” The President bears ultimate responsibility to ensure that this obligation is fulfilled. In practice, this means “that the committees should be advised of important new program initiatives and specific activities that have major foreign policy implications . . . to the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods and other exceptionally sensitive matters.”

While the exception for protection of sources and methods might seem at face value to represent a gaping loophole in the oversight scheme, legislative history indicates that Congress and the President understood that the circumstances under which “certain sensitive aspects of operations or collection programs” would not be divulged to Congress are “extremely rare.” There is some evidence to suggest that as a matter of practice the executive branch may limit disclosure on a “need-to-know” basis for certain intelligence information—perhaps to the chairmen and ranking members of the intelligence committees. In any event, the point of emphasis here is that this legislative oversight mechanism exists for all significant anticipated intelligence activities, and that the President, the DNI, and the heads of IC agencies bear joint responsibility for reporting such activities.

ii. Covert Action

---

Much has been written about the history and legality of CIA covert action, and most of it lies beyond the scope of this paper. For present purposes it will suffice to observe that covert action has been and continues to be an element of U.S. foreign policy that is explicitly authorized and regulated by statutory guidelines. Executive Order 12333 makes CIA the lead—though not exclusive—agency with authority for conduct of covert actions. Importantly, if the President determines that another agency—for example, NSA—is better suited to achieving a particular operational objective, he can direct that agency to conduct the covert operation. The Intelligence Authorization Act of 1991 codifies many of the provisions in Executive Order 12333, setting forth the procedures for authorization and conduct of covert actions. In keeping with prior statutes, the Act provides that a covert action must be authorized by the President after a finding that it is “necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.”


29 See generally A. John Radsan, An Overt Turn on Covert Action, 53 St. Louis U. L.J. 485 (2009). There is some debate as to whether the President has independent power under the Constitution—whether as Commander-in-Chief or as part of his duty to ensure that the laws are faithfully executed—to conduct covert action without legislative authorization. While this debate lies outside the present discussion, it is noteworthy that “[a]s a matter of practice, at least since President Jefferson, the executive has conducted covert action without specific congressional authorization, and at other times has gone beyond what authorization was given.” W. Michael Reisman & James E. Baker, Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law 118 (1992).

30 Exec. Order No. 12,333, 46 Fed. Reg. 59941, at 1.8(e) (Dec. 4, 1981) (providing that no agency other than CIA may conduct covert actions “unless the President determines that another agency is more likely to achieve a particular objective”).

31 Id. See also Mark R. Shulman, Discrimination in the Laws of Information Warfare, 37 Colum. J. Transnat’l L. 939, 947 (1999); Reisman & Baker, supra note 29, at 119 (observing that the covert action statute “effectively leaves the [choice of agency] up to the President”).


33 For a discussion of the legal history preceding the Act, see Radsan, supra note 29, at 517–31.

34 FY1991 Act §§ 602(a)(2), 503(a) (codified at 50 U.S.C. § 413b(a) (2005)).
While congressional approval is not required as a condition precedent to the authorization of a covert action, a number of procedures must be followed. Among these are requirements that presidential findings be in writing,\textsuperscript{35} that they be reported to the House and Senate intelligence committees\textsuperscript{36} or, if extraordinary circumstances so demand, to the “Gang of Eight” in Congress (consisting of the chairmen and ranking minority members of the intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate),\textsuperscript{37} and that this be done “as soon as possible” after presidential approval and “before the initiation of the covert action.”\textsuperscript{38} In the event that time does not allow for briefing prior to commencement of the covert action the President has approved, a written finding must be made within forty-eight hours of the start of the action.\textsuperscript{39} Presidential findings must specify the U.S. agencies involved and any non-U.S. government third parties which will fund or participate in the action.\textsuperscript{40} Findings may not authorize actions that violate the Constitution or U.S. statutes.\textsuperscript{41}

In addition to the purposive test contained in the statutory definition covert action—\textit{i.e.}, whether an operation’s objective is to influence political, economic, or military conditions abroad and whether the United States wishes to maintain plausible deniability as to its role in the operation\textsuperscript{42}—covert action can also be defined “by contradistinction to other activities.”\textsuperscript{43} The statutory definition of covert action explicitly excludes certain operations, thus exempting them from the relatively stringent oversight requirements outlined above. Covert action does not

\textsuperscript{35} 50 U.S.C. § 413b(a)(1) (FY1991 Act § 503(a)(1)).
\textsuperscript{36} Id. § 413b(c)(1) (FY1991 Act § 503(c)(1)).
\textsuperscript{37} Id. § 413b(c)(2).
\textsuperscript{38} Id. § 413b(c)(1).
\textsuperscript{39} Id. § 413b(a)(1).
\textsuperscript{40} Id. § 413b(a)(4).
\textsuperscript{41} Id. § 413b(a)(5).
\textsuperscript{42} See supra note 14 and accompanying text. See also Radsan, supra note 29, at 535 (“The essence of covert action lies in hiding the American hand behind an operation, not simply covering up some of the fingers.”).
\textsuperscript{43} Radsan, supra note 29, at 535.
include, *inter alia*, “activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities.” However, such activities, including “traditional” counterintelligence and those the “primary purpose” of which is collection, “do not lend themselves to precise definition.” As will be discussed in Part IV, the onset of network-based intelligence activities may confound the “primary purpose” distinction contained in the covert action statute.

2. Defensive Regulation

i. Espionage

A number of U.S. statutes proscribe and provide for punishment of espionage against the United States. These include laws prohibiting the collection, receipt, or transfer of “information respecting the national defense,” where the individual acts “with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation.” These defensive statutes also prohibit persons with authorized or unauthorized access to defense information from sale, transfer, or negligent loss of such information. They criminalize collection, including photography and use of aircraft, as well as disclosure of

---

44 Id. § 413b(e)(1) (emphasis added). “Traditional military activities” are also excluded from the scope of covert actions. Id. § 413b(e)(2). At first blush this exemption might seem to raise doubts about the need for any cyber operations that call for Department of Defense resources—for example, within the National Security Agency—to be authorized by findings and overseen as covert actions. However, legislative history makes clear that Congress intended to include in the definition of traditional military activities only those conducted “by military personnel under the direction and control of a United States military commander . . . preceding hostilities which are anticipated . . . involving U.S. military forces, or where such hostilities are ongoing, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.” S. Rep. No. 102-85, at 239. That history also suggests that Congress’s exclusion of traditional military activities does not negate the possibility for CIA-NSA collaboration in covert actions. See H. Rep. No. 102-166, at 29–30 (1991) (Conf. Rep.). Nor would it preclude NSA from being the sole agency responsible for a cyber covert action. *See supra* notes 30–31 and accompanying text.

45 Id.

46 18 U.S.C. § 793(a)–(c).


classified information to harm the United States or benefit a foreign government.\footnote{18 U.S.C. § 796.} Foreign agents are prohibited from receiving or attempting to receive classified information from any U.S. government officer or employee.\footnote{18 U.S.C. § 798.}

To supplement these laws, Congress passed the Economic Espionage Act (EEA) in 1996.\footnote{50 U.S.C. § 783(b) (2006).} This legislation outlaws the possession, collection, duplication, transfer, or sale of trade secrets for purposes of using the secret to benefit a foreign nation or any non-U.S. person.\footnote{Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488, § 1 (codified at 18 U.S.C. §§ 1831–1839 (2006)).} In addition, the EEA grants the Department of Justice broad authority to enforce the law extraterritorially.\footnote{See id.}

A common thread among these counterespionage statutes is their aim to punish acts that bear characteristics of \textit{theft} and \textit{exploitation} of state secrets. Put differently, they are addressed to traditional forms of intelligence collection rather than the features of influence and coercive force more readily associated with covert action.

ii. \textit{Covert Action}

There are no domestic laws that explicitly govern American responses vis-à-vis covert actions against the United States. To the extent that a covert action conducted by a foreign power may violate federal criminal statutes such as those outlawing material support to terrorism\footnote{See 18 U.S.C. §§ 2339A, 2339B (2009).} or proscribing the coercion of political activity,\footnote{See, e.g., 18 U.S.C. § 610 (1996).} the federal criminal system offers a number of tools for prosecuting that illegal activity. To the extent that offenses the U.S.
government deems to be covert actions induce it to project a response beyond our borders (and
external to the criminal justice context), such reactions are governed primarily by international
law, to which we now turn.

B. International Law

1. Offensive Regulation

i. Espionage

Although states and scholars have occasionally raised concerns about the legality of
peacetime intelligence collection under international law, states generally seem to accept the
practice as a legitimate function of a nation-state.58 The UN Charter protects states from
violations of their territorial integrity and political independence involving the threat or use of
force.59 Concerns have been raised that some forms of intelligence gathering may transgress this
right and violate the norm, also fundamental to the UN Charter, of peaceful cooperation among
states.60 However, international law has very little to say about the peacetime practice of

58 See Jeffrey H. Smith, Keynote Address: State Intelligence Gathering and International Law, 28 Mich. J. Int’l L. 543, 544 (2007) (“[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of
states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary
international law. Evidence of that is that when intelligence officers are accused of operating under diplomatic
cover in an embassy, they are nearly always declared personae non gratae and sent home. In exercising the right to
‘PNG’ a diplomat, the receiving state typically says their activities were inconsistent with diplomatic activities. I can
recall no instance in which a receiving state has said that these activities violate international law.”); see also Glenn
59 UN Charter art. 2, para. 4.
60 See Quincy Wright, Espionage and the Doctrine of Non-Intervention in Internal Affairs, in Essays on Espionage
and International Law 3, 12 (Roland J. Stranger ed., 1962). See also Ingrid Delupis, Foreign Warships and
law, even if it does not involve any ‘trespass’; espionage appears to be illegal under international law in time of
peace if it involves the presence of agents sent clandestinely by a foreign power into the territory of another state.
Such operations offend the principle of peaceful cooperation of states.”). Delupis qualifies her view by explaining
that espionage, though contrary to international law, is not an international crime—i.e., an offense indictable by
international tribunal—unless “accompanied by other acts.” Even then, however, Delupis claims that necessity or
self-defense arguments could “nullify” the illegality of the conduct. Id. at 68. For an embodiment of the norm of
peaceful interstate cooperation, see UN Charter, art. 1.
Since international law neither clearly condones nor explicitly proscribes the conduct, this would tend to support the conclusion that “[e]spionage is nothing but the violation of someone else’s laws.”

As Professor Simon Chesterman has explained, there are at least four bodies of international law that purport to regulate the conduct of espionage indirectly: norms of nonintervention, rules pertaining to diplomatic and consular relations, arms control treaties, and multilateral intelligence sharing agreements. With regard to nonintervention, the foundational rules of sovereignty may provide a measure of guidance with respect to the international-law limits, if any, on intelligence collection that falls short of an armed attack or explicit violation of other international norms. As articulated by the Permanent Court of International Justice in the 1927 *Lotus* case, “the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State.” According to Chesterman, this rule prohibits

---

61 See Richard A. Falk, *Foreword* to *ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW*, at v (Roland J. Stanger ed., 1962) (“Traditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture.”). As John Radsan has noted, “[t]hose words remain a fair assessment of the state of the literature today.” Radsan, *supra* note 7, at 602. *See also* Chesterman, *supra* note 3, at 1072, n.4 (noting that, aside from a handful of classified agreements involving intelligence-sharing among allies, and despite its importance to the conduct of international relations, there are few if any treaties that deal with espionage directly).


63 U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence, Part 5: Hearings Before the H. Select Comm. on Intelligence, 94th Cong. 1767 (1975) (statement of Mitchell Rogovin, Special Counsel to CIA Director). *See also* Cdr. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218–226 (1999) (concluding that territorially intrusive intelligence collection by U.S. agents is not a violation of *jus cogens* norms or other international law, and indeed may be a lawful exercise of the right of self-defense).

64 See Chesterman, *supra* note 3, at 1077.

65 *Id.* at 1081.

66 The Case of the S.S. “Lotus” (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 at 18 (Sept. 7).
unauthorized entry into and unauthorized use of territory, though the content of these proscriptions remains ambiguous.

Moreover, the question of how far a state’s “territory” extends remains unanswered. The UN Convention on the Law of the Sea prohibits intelligence collection by ships operating in the territorial waters of another nation, which extend up to twelve nautical miles from the coast, though it does not prohibit such collection on the high seas. The Outer Space Treaty does not prohibit collection using orbiting satellites. And indeed, despite expressions of concern and pragmatic responses to interception of electronic communications, nowhere in treaty law are such forms of SIGINT explicitly prohibited.

The international law of diplomatic and consular relations implicitly acknowledges the tradition of intelligence collection by foreign agents operating under diplomatic cover. Some provisions of the Vienna Convention on Diplomatic Relations (VCDR) seem directed at constraining espionage activity. For example, diplomats have obligations to respect the

---

67 See Chesterman, supra note 3, at 1082.
68 Chesterman does not confront this ambiguity beyond noting that certain acts, such as abductions and extraordinary renditions, would be unlawful under this norm. Id. For an apparent concurrence with this interpretation as to extraordinary rendition, see Robert M. Chesney, Leaving Guantánamo: The Law of International Detainee Transfers, 40 U. RICH. L. REV. 657 (2006). But see John Yoo, Transferring Terrorists, 79 NOTRE DAME L. REV. 1183, 1234 (2004) (contest ing “the mistaken assumption that domestic and international law significantly limit the transfer of captured enemy combatants”).
71 See Chesterman, supra note 3, at 1086–87. See also International Telecommunication Convention art. 22, Oct. 25, 1973, 1209 U.N.T.S. 255 (providing that states “reserve the right to communicate [international telecommunications] correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties”).
72 See id. at 1087–88.
73 See id. at 1088 (“The receiving state may limit a mission’s size and composition, and its consent is required to install a wireless transmitter or establish regional offices. The freedom of movement of diplomats may be restricted for reasons of national security.”).
internal laws of their receiving states, to avoid interference with those states’ internal affairs, and to refrain from using the premises of their missions “in any manner incompatible with the functions of the mission.” 74

Arms control agreements and multilateral intelligence sharing arrangements further support the view that intelligence collection is both necessary and lawful in at least some contexts. As Chesterman observes, the Anti-Ballistic Missile Treaty and the SALT I Agreement both provide for “national technical means of verification” of treaty compliance. 75 These and subsequent arms control agreements “effectively establish a right to collect intelligence, at least with respect to assessing compliance with the arms control obligations.” 76 Likewise, a number of (often classified) multilateral intelligence sharing arrangements such as the relationship among the signals intelligence agencies of the United States, United Kingdom, Australia, Canada, and New Zealand—the “five eyes”—may help to establish or evidence customary norms for what constitute acceptable forms of espionage. 77

If there is a conclusion to be drawn from this body of evidence, it is that international law in its current mode remains open to the possibility of lawful espionage. The lack of clarity in treaties and customary norms, combined with a proliferation of state practice, favors the conclusion that international law does not prohibit intelligence collection in the territory of other states. If this is the case, then espionage is indeed a (mere) violation of another state’s laws. 78

ii. Covert Action

75 Chesterman, supra note 3, at 1090–91.
76 Id. at 1091. Chesterman cites the Intermediate Range Nuclear Forces Treaty and the Open Skies Agreement as additional arms control treaties following this same approach of enforcing the agreement through intelligence collection.
77 See id. at 1093–98.
78 See supra note 63 and accompanying text.
The status of covert action under international law is at least as uncertain as the status of espionage. Taking a “fatalist position,” legal scholars “mostly conclude that covert action must be taken for granted.” However, the norm of nonintervention reflected in the UN Charter may implicitly prohibit subversive actions by one state in the territory of another during peacetime. But as Jeffrey Smith has observed, while this norm may be fundamental, “it is also fairly tattered. States seek to influence each other daily. Sometimes this is done by economic sanctions, or by international political pressure. Most of that activity is clearly legal . . . .” Put simply, there is no bright-line rule regarding the legal status of covert actions: some may be lawful, others unlawful.

The criteria for determining the lawfulness of covert actions are contestable. Dieter Fleck suggests that a covert action may be illegal if (1) it involves unauthorized entry into a foreign state’s airspace or territory, (2) it represents an “illegal exercise of jurisdiction on foreign territory,” (3) it is an attempt to destabilize a government, or (4) it entails common crimes such as a breach of data protection laws. On the other hand, Article 51 of the UN Charter states that “nothing in the present Charter shall impair the inherent right of self-defense.” Given this language granting apparently overriding authority to states’ sovereign rights of self-defense, a given covert action may represent a lawful exercise of this right, perhaps even if it involves use of force that would otherwise violate a nation’s territorial integrity and political independence as protected under Article 2(4) of the Charter.

---

80 See id.
81 Smith, supra note 58, at 545.
82 See generally Reisman & Baker, supra note 29.
83 Fleck, supra note 79, at 692–93.
84 UN Charter art. 51.
85 UN Charter art. 2(4) (“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 other manner inconsistent with the Purposes of the United Nations.”). To the extent the state claiming self-defense is invoking it as a collective right,
Recognizing the utter lack of clarity in the law, Professors Reisman and Baker propose the following test for assessing the legality of any proactive covert operation: “[1] whether it promotes the basic policy objectives of the Charter, for example, self-determination; [2] whether it adds to or detracts from minimum world order; [3] whether it is consistent with contingencies authorizing the overt use of force; and [4] whether covert coercion was implemented only after plausibly less coercive measures were tried.”^86 They add that any covert action must comply with the requirements of international humanitarian law (IHL, or law of armed conflict (LOAC)), such as proportionality and discrimination.\(^87\) That view seems to comport with the conventional legal interpretation under which the U.S. government gauges covert actions.\(^88\) And while their multi-factored test is not necessarily authoritative, Reisman and Baker provide a helpful point of departure for the impending discussion concerning the cyber context.

2. Defensive Regulation

i. Espionage

As one would expect given the ambiguous status of espionage under international law, there are no explicit defensive legal remedies in international legal tribunals or other

---

86 REISMAN & BAKER, supra note 29, at 77. The authors propose a similar test for assessing the legality of covert countermeasures, or exercises of the “non-belligerent right of armed reprisal.” See Derek Bowett, Reprisals Involving Recourse to Armed Force, 66 AM. J. INT’L L. 1 (1972). According to Reisman and Baker, “[a]lthough there is a generally recognized duty to seek reparation, or make a prior demand (necessity) before undertaking countermeasures, nowhere in current case law and commentary is there found a corollary requirement that the victim state provide prior notice of the specific countermeasure itself.” REISMAN & BAKER, supra note 29, at 115.

87 Id.

88 NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES § 4.2.1 (William A. Owens et al. eds., 2009) (“According to Jeff Smith, former general counsel to the Central Intelligence Agency (1995-1996), traditional U.S. interpretations of the laws of armed conflict . . . require covert action, whether or not it involves violent activities, to be conducted consistent with LOAC’s requirements.”).
international fora for punishing acts of espionage. While there exists no convention that clearly states the legal measures national governments may take to protect against espionage, states have residual authority to exercise extraterritorial jurisdiction over acts by non-nationals directed against their security, including acts of espionage. The VCDR also grants absolute discretion to terminate diplomatic relationships at will—i.e., to declare foreign diplomats personae non gratae and expel them without having to provide an explanation. Thus, there would seem ample grounds under international law for states’ efforts to defend against espionage by other states, without prohibiting states from engaging in espionage themselves.

ii. Covert Action

A state invoking the authority of international law as a remedial defense against covert action undertaken by another state is faced with a formidable task. Beyond qualifying the covert action as a violation of an international legal obligation, the state must be able to attribute the covert action to a specific foreign power. By the very nature of covert actions, efforts at attribution will often fail. As indicated in the following discussion, this problem becomes all the more vexing when the activity one attempts to attribute is network-based.

---

89 Even commentators who argue for the illegality of peacetime espionage under international law have largely been unable to identify specific international judicial remedies. See, e.g., Delupis, supra note 4, at 67–68.
90 Chesterman, supra note 3, n.43. See also RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(3) (1987) ("[A] state has jurisdiction to prescribe law with respect to . . . certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests."). The commentary to the Restatement explains: “International law recognizes the right of a state to punish a limited class of offenses committed outside its territory by persons who are not its nationals—offenses directed against the security of the state or other offenses threatening the integrity of governmental functions that are generally recognized as crimes by developed legal systems, e.g., espionage, counterfeiting of the state’s seal or currency, falsification of official documents, as well as perjury before consular officials, and conspiracy to violate the immigration or customs laws.” Id. cmt. f (known as the “protective principle”).
91 Vienna Convention on Diplomatic Relations art. 9(1).
93 See Fleck, supra note 79, at 695. I omit from discussion the further complications arising out of the “effective control” and “overall control” tests for state responsibility that have emerged from the decisions of international
C. Conclusions

The foregoing survey of domestic and international law reveals a remarkable degree of ambiguity. The offensive conduct of espionage is not explicitly prohibited as a matter of international law, though U.S. statutes provide a framework under which it is clearly lawful. At the same time, the United States and other countries seek to criminalize espionage against their own governments as a means of defending against and deterring the practice. The relatively rigorous criteria under which covert action is lawful are expressly set forth in U.S. statutes, though there is no such agreed-upon test under international law. At a minimum, U.S.-directed covert actions undergo executive-branch review for compliance with IHL. The law thus conceptually places covert action in a category of coercion, use of force, and armed attack (though any particular covert action may not bear every one of these features). Conversely, espionage is conceptualized under domestic and (to the extent it applies) international law to connote theft, exploitation, and surveillance. The remainder of this paper explores the degree to which collection of intelligence using cyber networks frustrates this conceptual distinction, blurring the boundaries between espionage and covert action to a degree that may require a rethinking of the legal framework under which such operations are conceived and overseen.

III. UNIQUE ASPECTS OF CYBER NETWORKS

Three features of cyberspace render it a unique medium for the conduct of espionage and covert action: the possibility of remote access, the difficulty of attributing intrusions and attacks to identifiable entities, and the difficulty of distinguishing between exploitation and attack.

---

tribunals in the Nicaragua and Tadic cases, respectively. See id. at 695–98. See also Nicaragua, 1986 I.C.J. 14; Prosecutor v. Tadic, Case No. IT-94-1-1 ICTY (Oct. 2, 1995).
Upon reflection, the third of these features appears to present particularly significant challenges for the conduct of espionage and covert action.

A. Three Distinctive Features

1. Remote Access

The first characteristic distinguishing cyberspace from traditional domains is remote access. In discussing the “changing nature of criminal espionage,” Susan Brenner and Anthony Crescenzi describe the remote access problem thus:

A key characteristic of traditional crime—proximity between victim and offender—is no longer a requirement for the targeting of sensitive critical infrastructure information. Spyware and keystroke loggers can be inserted into networks by insiders or by Trojan software downloaded surreptitiously and written for the express purpose of permitting remote access to sensitive data present on information networks.\(^94\)

Spies need not be physically located near sensitive information, or even in the nation to which that information belongs, in order to hack into critical networks and steal secrets. Once a computer is compromised by, for example, a Trojan horse software program,\(^95\) an unauthorized user can take control of the infected computer and steal data on the machine or configure it to become part of a botnet that automatically infects other machines.\(^96\)

2. Attribution Problem

A second unique characteristic of cyber activity is known as the attribution problem. The core of the problem is that cyber intrusions and attacks can be launched largely in secret, such

---


\(^95\) “A Trojan horse is a type of malicious software that fools a computer user into thinking that it will perform a wanted function but instead gives unauthorized access to the infected machine to a third party.” Wolfgang McGavran, Intended Consequences: Regulating Cyber Attacks, 12 Tul. J. Tech. & Intell. Prop. 259, 263 (2009). See also U.S. Computer Emergency Ctr., Targeted Trojan Email Attacks (2005), http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

that the identities of the actors behind them cannot readily be determined.97 “For example, a cyber attack seemingly originating in China might have been launched by the Chinese government, by some unofficial group of hackers in China or elsewhere, or by terrorists in the Middle East who disguise their identities.”98 In addition to identifying the responsible party, determining whether a given cyber intrusion was intentional or inadvertent is wrought with difficulty.99

3. Exploitation/Attack Quandary

A third distinctive aspect of cyber operations is the thorny issue of distinguishing between a cyber intrusion that constitutes theft or exploitation as opposed to an intrusion that rises to the level of “armed attack.” States are at pains to distinguish between acts of cyber espionage (“the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information”)100 and information war (“cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception”).101 I will refer to this problem as the exploitation/attack quandary (EAQ). Cyber attack can usefully be conceived of as “the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or

---

97 Richard L. Kugler, Deterrence of Cyber Attacks, in CYBERPOWER AND NATIONAL SECURITY 309, 317 (Franklin D. Kramer et al. eds., 2009).
98 Id. (noting that “[t]he alleged but ambiguous Russian cyber attack on Estonia is another obvious example” of the attribution problem at work).
100 Irving Lachow, Cyber Terrorism: Menace or Myth?, in CYBERPOWER AND NATIONAL SECURITY 437, 440 (Franklin D. Kramer et al. eds., 2009).
101 Id. at 441. Ontologically, this bifurcation is likely something of an oversimplification. Lachow, for example, suggests that at least three additional categories should be included: cyber crime, cyber terrorism, and “hacktivism.” See id. at 438–441. However, in order to focus the inquiry on the narrow questions I am seeking to address, the either/or distinction will be most useful.
networks.” The similarities between attack and exploitation in the cyber domain run deep: “Like cyberattack, a successful cyberexploitation requires a vulnerability, access to that vulnerability, and a payload to be executed—the only difference is in the payload to be executed.” In the case of cyber espionage, the payload might be a device that monitors and steals information, while in the case of cyber attack, the payload might be a virus that causes system failure.

At a fundamental level, the EAQ is intertwined with a definitional lacuna. There is no clear consensus as to whether the method for qualifying an act as a cyber attack or cyber exploitation should be derived (1) from the instrumentality used in launching it, (2) from an assessment of the characteristics of the infrastructure targeted, or (3) from the consequences of the act. While the consequence-based approach is preferred by the U.S. Department of Defense, international law remains ambiguous on the issue. Compounding this lack of clarity are two problems that go to the heart of the distinction difficulty: the crown jewels problem and the prospect of knock-on effects.

i. Crown Jewels Problem

A cyber intrusion may be characterized as “going after the crown jewels” when it employs “small-scale operations against a specific computer or user whose individual compromise would have enormous value,” such as a government’s nuclear command and control system or a high-ranking official’s laptop computer. In such a scenario, the perpetrator of the intrusion could presumably act with the intention (or “primary purpose”) of collecting

102 TECHNOLOGY, POLICY, LAW, AND ETHICS, supra note 88, § 1.4.
103 Id. § 1.4.
106 TECHNOLOGY, POLICY, LAW, AND ETHICS, supra note 88, §§ 2.6.4.2, 2.2.3.
intelligence on the target through surreptitious compromise of the target’s computer or system. But if the target were to become aware that its system had been compromised, it might view the theft of its information not as a mere act of exploitation but rather as an armed attack. For example, a government that utilizes a target-characteristic test to distinguish an act of cyber espionage from an act of information warfare might view the compromise of its nuclear command and control system as an act of warfare (since that system is presumably among its most sensitive and valuable security assets), even as the perpetrator of the intrusion intends merely to collect intelligence on the system. A government that utilizes an effects-based test in such a scenario might similarly view the effects of a system compromise as an affront to national security and sovereignty equivalent to armed attack, or it might—if confident in its analysis of the full scope of the compromise—view the effects as those constitutive of mere espionage.

In a recent analysis of cyber attack and exploitation, participants in a National Research Council study explained the problem thus:

Cyberexploitations are different from cyberattacks primarily in their objectives and in the legal constructs surrounding them. Yet, much of the technology underlying cyberexploitation is similar to that of cyberattack, and the same is true for some of the operational considerations as well. A successful cyberattack requires a vulnerability, access to that vulnerability, and a payload to be executed. A cyberexploitation requires the same three things—and the only difference is in the payload to be executed. . . . These technical similarities often mean that a targeted party may not be able to distinguish easily between a cyberexploitation and a cyberattack—a fact that may result in that party’s making incorrect or misinformed decisions.\(^{107}\)

This prospect that a target of cyber intrusion will interpret a given exploitation as a more aggressive act than the targeting party intends the intrusion to be raises serious questions, explored more fully in Part IV, about the level of prudence the party launching the exploitation

\(^{107}\) Technology, Policy, Law, and Ethics, supra note 88, § 2.2 (emphasis added).
should exercise in minimizing the possibility of “misinformed decisions” by the adversary while preserving the need for plausible deniability in such an event.

Further modeling of how the crown jewels problem highlights the conceptual imprecision precipitated by cyber networks merits consideration. For example, as Professor Dan Geer has explained, one of the unique problems of cybersecurity is that “the original owner continu[es] to possess stolen data after the thief takes it.”108 This problem may further erode the distinction between cyber exploitation and cyber attack to the extent that the distinction is grounded in a view of attack as tangibly destructive. To wit, a nation’s crown jewels need not be physically annihilated in order to be rendered useless.

ii. Knock-On Effects

An additional factor complicating the EAQ is the fact that cyber attacks can result in second- and third-order consequences, sometimes referred to as “knock-on effects.” As Scott Borg explains, three embedded vulnerabilities in the United States’ information-based economy leave us susceptible to targeted exploitations of those vulnerabilities.109 Redundancies, or the fact that many systems (e.g., cars or trains) can substitute for other systems (e.g., planes) by performing similar functions (transportation), leave the economy vulnerable to intensifier effects, which result from simultaneous attacks on different systems or businesses performing similar functions that could otherwise substitute for each other.110 Interdependencies, characterized by value chains in which one business activity feeds another, leave us susceptible to cascade effects, which result from attacks on business operations so interdependent that the interruption of one

110 Id. at 66.
interferes with another, and so on. Ne.
on platforms of cyber attack. It may take time for the consequences of such an attack to unfold, and as they do begin to appear, state actors may face severe difficulty in tracing data sets (e.g., of declining economic statistics) to their root causes in a cyber attack targeting a specific vulnerability. In sum, because knock-on effects can be severe and difficult to attribute to a specific cyber event, the process of using the perceived consequences of a known cyber intrusion to qualify that intrusion as either espionage or attack—as would take place under the legal framework advocated by the Department of Defense and a number of leading experts\textsuperscript{117}—could be error-prone and riddled with uncertainty.

B. Relative Significance of the EAQ

To be sure, the three problems identified here—remote access, attribution, and the EAQ—are interrelated. However, focus on the EAQ may yield unique insights for analyzing the conceptual distinction between espionage and covert action. With the establishment of a well-developed global architecture of signals intelligence already in place for some time, remote access is not a novel feature of espionage. Resorting to expulsion of a foreign agent who is discovered to be operating within one’s borders is not an option available to states in circumstances where the existence of foreign-based surveillance by way of electronic intercept is discovered, but states have likely structured their policies over the years so as to account for this reality.

The attribution problem is indeed vexing, enough so that it has been deemed by many to be the fundamental problem in cyber security.\textsuperscript{118} Nonetheless, the difficulty of identifying one’s

\textsuperscript{117} Many experts have suggested that an effects-based test for distinguishing attack from exploitation is the most plausible and desirable framework for understanding cyber attack. \textit{See, e.g., TECHNOLOGY, POLICY, LAW, AND ETHICS supra} note 103, at 1.6; Davis Brown, \textit{A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict}, 47 HARV. INT’L L.J. 179 (2006); Scott J. Shackelford, \textit{From Nuclear War to Net War: Analogizing Cyber Attacks in International Law}, 27 BERKELEY J. INT’L L. 192, 251 (2009).

\textsuperscript{118} \textit{See, e.g., Todd, supra} note 99, at 67 (identifying attribution and espionage as “the most challenging aspects of cyberspace”); Shackelford, \textit{supra} note 117, at 233 (describing the “crucial issue of attribution” and declaring that
adversary would seem an inherent (and hardly overlooked) feature of espionage from time immemorial. One would hope that, as it has vis-à-vis traditional attribution problems in the counterintelligence field, the United States will develop increasingly robust capabilities for identifying cyber perpetrators through all-source intelligence and technological advancements. In any event, compelling arguments can be adduced in support of the view that the scope of the attribution problem has been overstated. As Franklin Kramer has explained, “[b]ecause states normally act for geopolitical reasons, a high-end cyber attack by a state [i.e., a serious attack rendering military or key financial systems inoperative] probably would occur in a context in which it might be possible to determine the source.” For the attacking state in this scenario to conceal its identity would risk preventing delivery of its intended message and decreasing the possibility that the attacked state would acquiesce to the attacking state’s underlying political and strategic agenda.

In light of these observations, this discussion sets aside the many issues surrounding remote access and attribution. Returning to the EAQ, the next Part explores its likely implications for the practice of cyber espionage under law.

IV. IMPLICATIONS OF THE EXPLOITATION/ATTACK QUANDARY

The difficulty of distinguishing between cyber espionage/exploitation and cyber warfare/attack entails a blurring of the legal and theoretical distinction between intelligence

“[a]ttribution of a cyber attack to a state is a, if not the, key element in building a functioning regime” of international cyber security regulation.)

119 See Kugler, supra note 97, at 337–38. I draw some support for this optimism from reports on the government’s progress in designing and implementing EINSTEIN 3, a monitoring and intrusion-detection system for government computer networks. See, e.g., Ellen Nakashima, Cybersecurity Plan to Involve NSA, Telecoms, WASH. POST (Jul. 3, 2009).


121 Kugler, supra note 97, at 317–18.
collection (espionage) and covert action. The core practical implication of this conceptual breakdown is that, as a matter of prudence, future network-based intrusions should increasingly be treated as covert actions by the United States—both as an *ex ante* offensive matter and as an *ex post* defensive matter. This Part begins with an application of this conclusion to offensive uses of espionage and covert action, then turning to consider the defensive legal framework.

Two working assumptions anchor the following discussion: first, that intelligence agencies will increasingly employ cyber exploitation and cyber attack capabilities to the extent such uses serve their policy objectives and comport with their legal obligations;\(^\text{122}\) second, that absent an international convention to the contrary, the executive branch will evaluate cyber intrusions using an effects-based test to determine whether they rise to the level of “armed attacks” or “uses of force.”\(^\text{123}\)

**A. Offensive Cyber Activities**

In conducting *ex ante* assessment of offensive cyber operations, an initial question the executive branch must answer is whether proposed conduct falls under the category of intelligence collection or covert action. As an academic matter, the answer will of course vary depending on the operation. Some programs may clearly constitute espionage while others will be properly understood as covert actions. However, in light of the EAQ and the often unpredictable consequences potentially attendant to cyber activities, a good number of cyber intrusions may blur the distinction between espionage and covert action. U.S. officials would be

---

\(^{122}\) *See TECHNOLOGY, POLICY, LAW, AND ETHICS, supra* note 88, § 4.3 (noting, in light of the public information available regarding cyberexploitation of business and personal information as well as the Department of Defense, that “it would be highly surprising if the U.S. intelligence community did not know about and make use of cyberexploitation when appropriate or helpful”).

\(^{123}\) *See supra* note 104 and accompanying text (noting that this is the view of DoD); *TECHNOLOGY, POLICY, LAW, AND ETHICS, supra* note 88, § 1.6 (“The committee’s view of the basic framework for the legal analysis of cyberattack is based on the principle that notions related to “use of force” and “armed attack” . . . should be judged primarily by the effects of an action rather than its modality. That is, the fact that an attack is carried out through the use of cyberweapons rather than kinetic weapons is far less significant than the effects that result from such use, where “effects” are understood to include both direct and indirect effects.”).
well advised to establish a policy subjecting operations that are not clearly confined to collection
to the heightened oversight procedures regulating covert action, even where the “primary
purpose” of such operations is espionage.

1. Domestic Regulation

As discussed in Part II, Congress in enacting the covert action statute adopted special
oversight procedures for operations that involve influencing political, economic, or military
conditions abroad and for which the United States wishes to maintain plausible deniability.\textsuperscript{124} These procedures exclude activities the “primary purpose” of which is intelligence collection. But as described in the foregoing analysis of the EAQ, even where the primary purpose of a
cyber exploitation is to collect intelligence, such operations may lead to many of the same
consequences that are contemplated in the statutory definition of covert action.

Cyber operations may influence the affairs of a foreign power or the relations between
that power and the United States in two ways. First, because cyber exploitations and cyber
attacks bear such a high degree of similarity, intrusions intended as cyber exploitations may be
interpreted by the adversary as attacks. Presumably the adversary’s reaction under such
circumstances would be commensurate with its interpretation, producing a result—perhaps even
as drastic as declaring war—that can only be described as “influencing political, economic, or
military conditions abroad.” As with other activities traditionally understood as covert actions—
e.g., covert paramilitary operations, propaganda, political action, and election support\textsuperscript{125}—this
would entail very much the species of results that Congress sought to regulate by subjecting
covert actions to careful oversight. Second, to the extent we have cause for concern about the
potential knock-on effects of a cyber exploitation, the prospect that those effects will influence

\textsuperscript{124} See supra notes 42–45 and accompanying text.
\textsuperscript{125} See S. REP. NO. 102-85, at 235.
political, economic, or military conditions abroad in unanticipated ways further counsels a heightened measure of *ex ante* caution with respect to authorization of such operations.

2. *International Law Model*

Treating an increased number of cyber exploitations as covert actions would account for the fact that cyber exploitations may be more appropriately analyzed under a law of armed conflict paradigm than a purely domestic-law model. The CIA and other intelligence agencies apparently review all covert actions, whether or not they involve violent activities, for compliance with LOAC. 126 Given the general difficulty of distinguishing cyber exploitation from cyber attack, the choice to evaluate such operations as if they were attacks—perhaps using Reisman & Baker’s four-pronged test for compliance with *jus ad bellum* and *jus in bello* discussed in Part II 127—would seem a prudent check on the danger that activity constituted as espionage might cross the line into unlawful warfare. Otherwise, the United States could be placed at risk if it conducted collection activities that created spillover effects or were interpreted as rising to the level of “armed attack” or “use of force” under international law.

3. *Limiting Opportunity Costs*

Subjecting an increasing number of intelligence collection operations to the special oversight provisions of covert action entails substantial opportunity costs. Indeed, in one sense it is counterintuitive to suggest an increase in the use of the covert action model with the onset of cyber operations, given the comparatively low cost at which such operations may be conducted 128 and the relative burden of presidential findings. The very fact that the statutory definition of covert action excludes activities with a primary purpose of intelligence gathering

---

126 See *supra* note 88 and accompanying text.
127 See *supra* notes 86–87 and accompanying text.
128 See TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 88, § 6.1.2 (“*[T]he acquisition cost of software-based cyberattack tools is almost entirely borne in research and development, since they can be duplicated at near-zero incremental cost.*”).
and those with a traditional counterintelligence function\textsuperscript{129} might seem tailor-made to establishing a broad program of cyber exploitation constituted as ordinary intelligence or counterintelligence activity. Moreover, in passing the FY1991 Intelligence Authorization Act, the Senate assumed that the covert action reporting requirements would not apply to activities “that may literally fall within the definitions [of covert action] but for which it would be impractical to seek Presidential approval and report to Congress on a case-by-case basis.”\textsuperscript{130} The impracticality of subjecting the entire scope of NSA and CIA network-based intelligence collection to covert action oversight requirements is, to be sure, beyond dispute. Finally, it might also be argued that since we have little evidence that our adversaries are exercising similar caution against us, treating more cyber espionage as covert action unnecessarily hamstrings the United States’ global intelligence collection mission at a critical time.

These legitimate concerns must be addressed in any attempt to construct a consistent oversight framework for cyber operations. Indeed, it is surely impractical for the National Security Council to be involved in decisions about individual cyber exploitations at a granular level and for intelligence agencies to seek regular presidential findings for such operations. As a solution, perhaps the oversight requirements of Executive Order 12333 could be fulfilled by subjecting certain broader classes of cyber exploitation to the covert-action finding and reporting requirements under the umbrella of a single covert action. This would allow for regular appraisal of such activities, including scrutiny of the degree to which the crown jewels and knock-on effects problems have or have not arisen in conjunction with a given type of operation. This more sweeping categorization of various intrusions under the auspices of a certain ongoing covert action could less easily be said to hamper the United States’ efforts to keep up with its

\textsuperscript{129} See supra note 44 and accompanying text.
\textsuperscript{130} S. REP. NO. 102-85, at 235.
adversaries in the cyber domain. To the extent it does constrain the profusion of certain intelligence operations, the rationales adduced above suggests that such constraints may be called for. Put simply, a measure of self-imposed restraint in this context is warranted, as such restraint could aid the avoidance of unanticipated negative results stemming from the nature of generative networks and layered vulnerabilities.

4. Drawing Lines

The foregoing discussion does not address the significant line-drawing problem created by this recommendation that more cyber exploitations be treated as covert actions. Defining the precise boundaries of which types of cyber exploitations should be classified as traditional intelligence collection, counterintelligence activity, or activity the “primary purpose” of which is to collect intelligence, and which types of exploitations should be viewed as covert actions because of their implications in light of the EAQ, is beyond the technical expertise of this author and the scope of this paper. It seems plausible, however, that such distinctions could be established within and across the executive branch as experience with various methods of cyber exploitation and attack mounts.

B. Defensive Cyber Activities

Just as the outcomes of offensive use of cyber entail uncertainty, it will not always be clear when the United States has been the victim of a cyber attack as opposed to cyber exploitation. Notwithstanding possible overstatement of the attribution problem, it also may be unclear which state or non-state actors are responsible for an attack or exploitation when it occurs. This reality demands an awareness of, among other issues, the prospect that latent knock-on effects could increase the magnitude of what may initially appear to be an act of exploitation. It demands that any legal paradigm for offensive cyber operations that increasingly
treats them as covert actions must be accompanied by similar treatment of cyber intrusions from a defensive perspective.

Two practical benefits accrue from treating known cyber exploitations against the United States as covert uses of force. First, doing so maximizes the legal flexibility of the government response to that act. Consider the relatively limited efficacy of the traditional counterespionage criminal statutes at the government’s disposal when applied to the cyber realm. In comparison, covert action would seem a potentially effective form of response where other traditional legal tools fall short. Assuming for purposes of discussion that the executive branch employs the Reisman & Baker test for legality of covert actions in the cyber domain, under that rubric the U.S. response to a cyber attack or exploitation against it could lawfully take the form of a covert action if (1) it promotes the policy objectives of the UN Charter, (2) it adds to minimum world order, (3) it is consistent with contingencies authorizing overt use of force, and (4) it is implemented only after plausibly less coercive measures have been tried. Treating more exploitations targeted against the United States as covert actions would place more of them in the *jus ad bellum* and *jus in bello* framework needed for application of this test for legality. For example, if notified that the President wishes to respond to a cyber intrusion with a covert action, executive branch lawyers would be better equipped to characterize that covert-action response as one that satisfies contingencies authorizing overt use of force (the third criteria in the Reisman & Baker legality test) if the initial intrusion were construed as a use of force against the United States.

The second practical benefit of defensively treating more exploitations as covert attacks would be to help focus the government’s attention and efforts on the critical need to integrate

---

131 See discussion *supra* Part II.B.2.i.
132 See *supra* note 86 and accompanying text.
offensive and defensive capabilities to conduct effective counterintelligence. To the extent that more cyber exploitations against the United States are viewed by the IC as covert actions, the executive branch may be more inclined to recognize that the best cyber defense is a good cyber offense, with covert action playing an integral role in the matrix. Noting that in this cyber game, “the contest between offense is dreadfully mismatched, with the advantage strongly in the offensive corner,” James Gosler calls for a cultural shift in the IC and a renewed willingness to increase investment so as to keep the upper hand. He explains the need thus:

By prudently increasing offensive investments and by better integrating human and technical collection elements, we can increase the price of admission into the top level of intelligence collection. By augmenting our offensive capabilities, we can operationally afford to eliminate vulnerabilities that can be exploited with less sophisticated techniques. This requires significant new investment in our defensive approach and a tight coupling of our defensive and offensive elements.

Coupling defensive and offensive elements entails a much broader range of reforms to current practice than can be addressed in this space. I would suggest only that the offensive use of covert action as a defense against exploitation of U.S. vulnerabilities might be more readily achieved by shifting the conceptualization of cyber intrusions against the United States to an increased emphasis on the possibility that they are covert acts of force rather than acts of espionage. While preserving domestic legal remedies for cases in which actors can be readily identified and prosecuted, a robust covert action program may be the most realistic strategy of deterrence and counterintelligence that the United States can hope for until the utopian day when

134 Id. at 103.
135 For a general discussion of offense-defense integration and other reforms in the counterintelligence arena, see generally James R. Gosler, Counterintelligence Too Narrowly Practiced, in VAULTS, MIRRORS AND MASKS: REDISCOVERING U.S. COUNTERINTELLIGENCE (Jennifer E. Sims & Burton Gerber eds., 2009).
we might rely on the goodwill and self-restraint of states to adhere to mutually agreed terms of international engagement absent an external enforcement structure.

V. CONCLUSION

This paper has focused on the question of how the exploitation/attack quandary may change the nature of espionage from a practical legal standpoint. The legal paradigm of covert action may be a more appropriate framework of oversight for conceptualizing, initiating, and responding to acts of exploitation and attack in the cyber domain. This is partly a hedge on the crown jewels and knock-on effects problems potentially attendant to such operations, but it also represents a measured endeavor to preserve flexibility among offensive exploitation and attack alternatives. The dearth of credible means of deterrence in this realm renders the need for such flexibility palpable. It is plausible that this conclusion would persist even if the attribution problem were to be largely resolved and states reached normative consensus on the definitions of “armed attack” and “use of force.” For unless and until the United States government can determine with confidence the degree to which it has been infiltrated when foreign states and non-state actors launch computer-network attacks and exploitations, the judicious exercise of covert power may be an indispensable tool in the state’s cyber arsenal.