(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action

*Robert D. Williams**

Abstract

This Article makes two related arguments: one descriptive and one normative. Descriptively, it contends that the use of computer networks in carrying out intelligence operations entails a blurring of the conceptual and legal distinction between intelligence collection and covert action. In light of this emerging reality, executive branch officials face an increasingly difficult choice of legal paradigms in conducting oversight of offensive intelligence operations, as well as in seeking to characterize and respond to cyber intrusions from a defensive standpoint. Normatively, the Article argues that, absent a legislative solution, the U.S. Government should adapt to this blurring of the legal lines by increasingly treating cyber intrusions as covert actions—even, in some cases, where the primary purpose of the operation is intelligence collection. This evolution in the practice and oversight of intelligence would serve as a check against the inherent uncertainty of consequences attendant to the use of cyberspace as a medium for clandestine intelligence operations. It would also account for the need to establish flexible and proactive deterrent options in a domain where traditional legal remedies are largely inadequate to manage the threats—and assets—of cyber exploitation and cyber attack.

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 tem-

* J.D., Harvard Law School, 2010. The author is grateful to Jack Goldsmith for his mentorship and helpful comments on a January 2010 draft. The author recently worked in the Office of Legal Counsel, United States Department of Justice. The views expressed in this Article, however, are those of the author and do not necessarily reflect the views of the United States Government.

1 *See, e.g.*, Arthur S. Hulnick, Keeping Us Safe: Secret Intelligence and Homeland Security 43 (2004); Simon Chesterman, *The Spy Who Came In from the Cold War: Intelligence and International Law*, 27 Mich. J. Int'l L. 1071, 1072 (2006). Historical accounts of espionage and other forms of intelligence collection date back more than 3000 years. *See* 1 Encyclopedia of Intelligence and Counterintelligence, at xv (Rodney P. Carlisle ed., 2005).

2 *Compare* Geoffrey B. Demarest, *Espionage in International Law*, 24 Denv. J. Int'l L. & Pol'y 321, 347 (1996) (concluding that espionage is an "unfriendly act" but not a violation of international law), *with* Manuel R. García-Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. Pitt. L. Rev. 65, 79–80 (1964) (arguing that

pering 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 yielded this cascade of "generativity" makes states vulnerable to acts of espionage and information warfare that threaten their economic and national security.[6]

This development raises a host of questions about the evolving nature of intelligence operations and their 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 Article focuses primarily on the third of these

---

"peacetime espionage is regarded as an international delinquency and a violation of international law").

3 *See* Chesterman, *supra* note 1, at 1072 (citing "sporadic demands for nonrepetition" of spying activities); *see also* Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, Annex, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/56/10, art. 30 (Dec. 12, 2001) (declaring that states responsible for "internationally wrongful act[s]" have obligations to cease the wrongful acts and "[t]o offer appropriate assurances and guarantees of non-repetition, if circumstances so require").

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* 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."); Chesterman, *supra* note 1, 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.").

5 For purposes of this Article, 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).

6 *See* EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, at iii (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 36–61 (2008) (discussing the "generative" nature of the Internet and tradeoffs between cyber security and innovation); Jack Goldsmith, Op-Ed., *Defend America, One Laptop at a Time*, N.Y. TIMES, July 2, 2009, at A23.

issues and its consequences for the treatment of cyber intrusions under U.S. and international law. It argues principally that the difficulty of distinguishing between cyber *exploitation* and cyber *attack* entails a blurring of the conceptual and legal distinction between intelligence collection and covert action. In light of this practical reality, intelligence lawyers in the information age will face increasingly difficult judgment calls in determining which legal paradigms to turn to as policymakers initiate and respond to intrusive acts in cyberspace.

Recognizing the opportunity costs associated with these choices, this Article suggests that prudence counsels for increasing treatment of network-based intrusions as covert actions rather than traditional espionage—i.e., as clandestine attempts to influence political, economic, or military conditions in other countries, rather than intelligence collection. This evolution in the practice and oversight of intelligence would represent a check against the inherent uncertainty attendant to the use of cyberspace as a medium for clandestine operations. It would also help satisfy the need for a flexible deterrent structure absent the availability of traditional legal remedies for managing the threats—and offensive assets—posed by cyber networks.

This Article proceeds as follows. Part I defines key terms and surveys the domestic and international laws governing peacetime espionage and covert action. Part II explains three features of network-based espionage that differentiate it from traditional espionage, focusing on the specific difficulty of distinguishing cyber exploitation from cyber attack. Part III identifies how this "exploitation/attack quandary" renders much of the existing legal treatment of espionage inapt or inadequate. In doing so, it suggests a tentative approach for the United States that would fit cyber intrusions within existing legal structures relating to covert action, a potentially 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 deterrent and retributive defense to cyber attack and exploitation while minimizing the risk that its own utilization of cyberspace oversteps the bounds of legality or generates negative consequences for national and international security.

I. 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. intelli-

gence collection and covert action find their roots in the National Security Act of 1947[7] and Executive Order 12,333.[8] Provisions criminalizing espionage against the United States are scattered throughout portions of Title 18 of the United States Code,[9] while many defensive responses to covert action—insofar as they involve the projection of power abroad rather than through domestic criminal proceedings—are governed by international law.[10] For its part, international law touches upon espionage only indirectly. The status of covert actions under transnational legal regimes is a subject of some debate, but 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.

What emerges in surveying this terrain is the sense that the law classifies espionage as a form of thievery and exploitation while placing covert action under a rubric of attack and coercive manipulation. This conceptual distinction supplies a basis for differing legal treatment of the two forms of intelligence activity, and carries unique implications for computer-network operations in the field of intelligence.

A. Definition of Terms

As a threshold matter, it is important to clarify precisely what is meant by the term "espionage," for it represents but one species of intelligence activity.[11] *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."[12] In line with this definition, for purposes of this Article, the terms "espionage" and "intelligence collection" will be used interchangeably and in contradistinction to "covert action."[13] With this definition as a starting

---

7 National Security Act of 1947, 50 U.S.C. §§ 401–442a (2006).

8 Exec. Order No. 12,333, 3 C.F.R. 200 (1982).

9 *See, e.g.*, 18 U.S.C. §§ 793, 794 (2006).

10 *See infra* Part I.B.2.b.

11 *See* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 599 (2007).

12 BLACK'S LAW DICTIONARY 585 (9th ed. 2009).

13 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 11, at 599 ("Covert action . . . does not fit into the traditional categories of collection and analysis at intelligence agencies."). Much writing on the subject, however, excludes 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

point, it will be helpful to consider the legal architecture of espionage from both offensive and defensive perspectives. With respect to the former, this Article 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.[14]

This working definition of espionage omits two categories of intelligence activity entrusted to the Intelligence Community ("IC")[15] by U.S. law: intelligence analysis and covert action.[16] Analysis involves making sense of the various pieces of information procured from human and technical sources around the world.[17] 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."[18] While intelligence analysis may be a practice rife with legal uncertainty,[19] such questions are not within the scope of this discussion. As we shall see, however, the utilization of cyber networks in carrying out collection

---

"espionage" as a practice of information collection warrants the working definition set forth here. *See, e.g.*, *Espionage Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/espionage (last visited Mar. 20, 2011) (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").

14 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 1, 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 Prisoner-of-War status unless they return to their armed forces and cease espionage activities prior to being captured. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) arts. 37(2), 46(4), *adopted* June 8, 1977, 1125 U.N.T.S. 3.

15 "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." *About the Intelligence Community*, INTELLIGENCE.GOV, http://www.intelligence.gov/about-the-intelligence-community/ (last visited Mar. 20, 2011).

16 *See* Radsan, *supra* note 11, at 599.

17 *See* ROB JOHNSTON, CENT. INTELLIGENCE AGENCY, ANALYTIC CULTURE IN THE U.S. INTELLIGENCE COMMUNITY (2005), *available at* http://www.fas.org/irp/cia/product/analytic.pdf.

18 50 U.S.C. § 413b(e) (2006).

19 *See, e.g.*, Chesterman, *supra* note 1, at 1073 (noting the potential intellectual property and privacy laws that may be implicated by intelligence analysis).

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 and nonstate actors while criminalizing espionage by foreign actors. The following discussion considers these offensive- and defensive-oriented laws regarding collection and covert action in turn.

1. Offensive Regulation

a. Espionage

Authority for 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,[20] as well as the many congressional appropriations for intelligence activities.[21] Authority for Congress's enactment of statutes governing U.S. intelligence collection is drawn from its constitutional power to "provide for the common Defence and general Welfare of the United States."[22] Through the NSAct, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004,[23] and other statutes, Congress conveys broad authority to the Central Intelligence Agency ("CIA") to "collect intelligence through human sources and by other appropriate means."[24] Crudely speaking, the NSAct confers legal authority for the stealing of foreign secrets. It also provides for, among other programs and agencies, the establishment of a signals intelligence program to be coordinated by the Secretary of Defense through the National Security Agency ("NSA").[25] Collectively, these elements comprise the National Intelligence Program overseen by the Director of National Intelligence ("DNI").[26] This set of provisions clearly authorizes the IC to engage in clandestine foreign intelligence collection.[27]

---

20 Central Intelligence Agency Act of 1949, 50 U.S.C. §§ 403a–403s (2006).

21 Radsan, *supra* note 11, at 601.

22 U.S. CONST. art. I, § 8, cl. 1.

23 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

24 50 U.S.C. § 403-4a(d)(1).

25 *See id.* § 403-5(b)(1).

26 *See id.* § 403(a)–(b).

27 *See* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTEL-

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 covert actions, "including any significant anticipated intelligence activity and any significant intelligence failure."[28] The President bears ultimate responsibility to ensure that this obligation is fulfilled.[29] In practice, this means "that the committees should be advised of important new program initiatives and specific activities that have major foreign policy implications,"[30] but only "[t]o 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."[31]

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."[32] There is some evidence to suggest that, as a matter of practice, the executive branch may limit disclosure of certain intelligence information on a "need-to-know" basis to the chairmen and ranking members of the intelligence committees.[33] 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 are jointly responsible for reporting such activities.

LIGENCE ACTIVITIES, FOREIGN AND MILITARY INTELLIGENCE, S. REP. NO. 94-755, bk. I, at 128–31 (1976).

28 50 U.S.C. § 413a(a)(1).

29 *Id.* § 413(a)(1).

30 S. REP. NO. 102-85, at 32 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 225.

31 50 U.S.C. § 413a(a).

32 This language draws from the Senate report accompanying the Intelligence Oversight Act of 1980, S. REP. NO. 96-730, at 6 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4192, 4197, to which the Senate report construing the intelligence-activity reporting provisions of the Intelligence Authorization Act, Fiscal Year 1991, refers. *See* S. REP. NO. 102-85, at 33, *reprinted in* 1991 U.S.C.C.A.N. at 226.

33 *See* ALFRED CUMMING, CONG. RESEARCH SERV., STATUTORY PROCEDURES UNDER WHICH CONGRESS IS TO BE INFORMED OF U.S. INTELLIGENCE ACTIVITIES, INCLUDING COVERT ACTIONS 4–5 (2006), *available at* http://www.fas.org/sgp/crs/intel/m011806.pdf; Nancy Pelosi, *The Gap in Intelligence Oversight*, WASH. POST, Jan. 15, 2006, at B7.

b. Covert Action

Much has been written about the history and legality of CIA covert action,[34] and most of it lies beyond the scope of this Article. For present purposes it will suffice to observe that covert action—that subset of secret activities to influence political, economic, or military conditions in other countries—has been and continues to be an element of U.S. foreign policy that is explicitly authorized and regulated by statutory guidelines.[35] Executive Order 12,333 makes the CIA the lead, though not exclusive, agency with authority for covert actions.[36] Importantly, if the President determines that another agency—for example, the NSA—is better suited to achieve a particular operational objective, he may direct that agency to conduct the covert action.[37] No matter which agency is responsible for the planning and execution of a covert action, the legal definition of that term "appl[ies] uniformly and equally to all elements of the U.S. Government."[38]

---

34 *See generally* WILLIAM J. DAUGHERTY, EXECUTIVE SECRETS: COVERT ACTION AND THE PRESIDENCY (2004); ROY GODSON, DIRTY TRICKS OR TRUMP CARDS: U.S. COVERT ACTION AND COUNTERINTELLIGENCE (Transaction Publishers 2001) (1995); JOHN JACOB NUTTER, THE CIA'S BLACK OPS: COVERT ACTION, FOREIGN POLICY, AND DEMOCRACY (2000); JOHN PRADOS, PRESIDENTS' SECRET WARS: CIA AND PENTAGON COVERT OPERATIONS FROM WORLD WAR II THROUGH THE PERSIAN GULF (Elephant Paperbacks rev. & expanded ed. 1996) (1986); JOHN PRADOS, SAFE FOR DEMOCRACY: THE SECRET WARS OF THE CIA (2006); JOHN RANELAGH, THE AGENCY: THE RISE AND DECLINE OF THE CIA (1986); EVAN THOMAS, THE VERY BEST MEN: FOUR WHO DARED: THE EARLY YEARS OF THE CIA (1995); GREGORY F. TREVERTON, COVERT ACTION: THE LIMITS OF INTERVENTION IN THE POSTWAR WORLD (1987); TIM WEINER, LEGACY OF ASHES: THE HISTORY OF THE CIA (2007).

35 *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 whatever 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).

36 Exec. Order No. 12,333, § 1.8(e), 3 C.F.R. 200, 205 (1982) (providing that no agency other than the CIA may conduct covert actions "unless the President determines that another agency is more likely to achieve a particular objective").

37 *Id.*; *see also* REISMAN & BAKER, *supra* note 35, at 119 (observing that Executive Order 12,333 "effectively leaves the [choice of agency] up to the president"); Mark R. Shulman, Note, *Discrimination in the Laws of Information Warfare*, 37 COLUM. J. TRANSNAT'L L. 939, 947 (1999).

38 S. REP. NO. 102-85, at 44 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 237.

The Intelligence Authorization Act of 1991[39] codifies many of the provisions in Executive Order 12,333, setting forth the procedures for authorization and conduct of covert actions.[40] 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."[41] While congressional approval is not required as a condition precedent to the authorization of a covert action, "Congress has the constitutional power to refuse to appropriate funds to carry out covert actions and may impose conditions on the use of any funds appropriated for such purposes."[42] Beyond this check from the Legislature, executive covert action is constrained by a number of procedures that must be followed. Among these are requirements that presidential findings be in writing,[43] that they be reported to the House and Senate intelligence committees[44] 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),[45] and that this be done "as soon as possible after [presidential] approval and before the initiation of the covert action."[46] 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.[47] Presidential findings must specify the U.S. agencies involved and any non-U.S. Government third parties that will fund or participate in the action.[48] Findings may not authorize actions that violate the Constitution or federal statutes.[49]

In addition to the purposive test contained in the statutory definition of covert action—that is, whether an operation's objective is to

---

39 Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, 105 Stat. 429 (codified in scattered sections of 10 and 50 U.S.C.).

40 For a discussion of the legal history preceding the Act, see Radsan, *supra* note 35, at 517–31.

41 50 U.S.C. § 413b(a) (2006).

42 S. REP. NO. 102-85, at 34, *reprinted in* 1991 U.S.C.C.A.N. at 227.

43 50 U.S.C. § 413b(a)(1).

44 *Id.* § 413b(c)(1).

45 *Id.* § 413b(c)(2).

46 *Id.* § 413b(c)(1).

47 *Id.* § 413b(a)(1).

48 *Id.* § 413b(a)(3)–(4).

49 *Id.* § 413b(a)(5).

influence political, economic, or military conditions abroad and whether the United States wishes to maintain plausible deniability as to its role in the operation[50]—covert action can also be defined "by contradistinction to other activities."[51] The statutory definition of covert action explicitly excludes certain operations, thus exempting them from the relatively stringent oversight requirements outlined above.[52] Covert action does not include, among other operations, "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."[53] By contrast, at the time Congress codified these exceptions, "covert paramilitary operations, propaganda, political action, election support and related activities" were all traditionally understood to be covert actions.[54]

The categories of non–covert action, including "traditional" counterintelligence and activities the "primary purpose" of which is collection, "do not lend themselves to precise definition."[55] Drawing lines between covert action and other forms of intelligence activity is a practice not easily grounded in statutory text. Congress emphasized, however, that its definition of covert action "focuses on the objective

---

50 *See* National Security Act of 1947 § 503(e), 50 U.S.C. § 413b(e); S. REP. NO. 102-85, at 43 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 236 ("The essential element of a covert action is that the role of the United States in the activity is not apparent and not intended to be acknowledged at the time it is undertaken. The United States, in other words, seeks a form of plausible denial to the outside world."); Radsan, *supra* note 35, at 535 ("The essence of covert action lies in hiding the American hand behind an operation, not simply covering up some of the fingers.").

51 Radsan, *supra* note 35, at 535.

52 50 U.S.C. § 413(b)(e)(1)–(4).

53 *Id.* § 413b(e)(1). "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—e.g., within the NSA—to be authorized by findings and overseen as covert actions. *Cf.* Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar,"* 22 FLA. J. INT'L L. 333, 359 (2010) (arguing that military-overseen cyber operations should not be subject to Congressional reporting requirements). Legislative history makes clear, however, that Congress intended to include in the definition of traditional military activities only those activities 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 46, *reprinted in* 1991 U.S.C.C.A.N. 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 the NSA from being the sole agency responsible for a cyber covert action. *See supra* notes 36–37 and accompanying text.

54 S. REP. NO. 102-85, at 42, *reprinted in* 1991 U.S.C.C.A.N. at 235.

55 Radsan, *supra* note 35, at 535.

features of the activity, rather than on a formal relationship to foreign policy purposes, as the controlling test in determining which activities constitute covert action."[56] In crafting the intelligence oversight structure, Congress thus expressed paramount concern with the *consequences* of actions carried out by the United States in secret. To be sure, the Legislature did not seek to draw within the ambit of "covert action" those operations such as intelligence liaison relationships, which produce intelligence indirectly; nor did it intend to subsume traditional counterintelligence missions such as double-agent operations and exposure of foreign agents under the umbrella of covert action—even where such operations influence the military plans of foreign powers.[57] But Congress was also explicit in underscoring that it did not intend "to create an avenue for designing operations to avoid the covert action requirements."[58]

As Professor John Radsan has explained, the drafting of the current definition of covert action was in many ways a response to fallout from the Iran-Contra Affair.[59] The definition thus "applies not only to classic covert actions (i.e., propaganda, paramilitary action, and political action), but also to some activities that do not fit the traditional rubric of foreign intelligence and counter-intelligence."[60] Again, of fundamental importance to Congress seems to have been the need to avoid negative consequences from an operation gone awry. Thus, one "way to define covert action is by the potential damage of a failed operation. In general, a failed covert action has more profound repercussions than a failed foreign intelligence [collection] operation."[61]

Having sketched the broad outlines of the U.S. legal framework applicable to offensive utilization of covert action, a picture begins to emerge with espionage, on the one hand, viewed through the lens of theft, surveillance, and exploitation of secrets; and covert action, on the other hand, viewed through the lens of clandestine coercion, force, and manipulation of events overseas. The task of distinguishing these two forms of intelligence activity will be taken up again in Part III. As will become clear in the course of discussion, the onset of network-based intelligence activities in the information age frustrates and con-

---

56 S. REP. NO. 102-85, at 43, *reprinted in* 1991 U.S.C.C.A.N. at 236.

57 *See id.* at 44–45, *reprinted in* 1991 U.S.C.C.A.N. at 237–38.

58 *Id.* at 44, *reprinted in* 1991 U.S.C.C.A.N. at 237.

59 *See* Radsan, *supra* note 35, at 529–36.

60 *Id.* at 536.

61 *Id.*

founds the already vague distinctions embedded in the covert action and espionage statutes.

2. Defensive Regulation

a. 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."[62] These defensive statutes also prohibit the sale, transfer, or negligent loss of defense information by persons with authorized or unauthorized access to such information.[63] They criminalize collection,[64] including by means of photography[65] and aircraft,[66] as well as disclosure of classified information for the purpose of harming the United States or benefitting a foreign government.[67] Foreign agents are prohibited from receiving or attempting to receive classified information from any U.S. Government officer or employee.[68]

To supplement these laws, Congress passed the Economic Espionage Act ("EEA")[69] in 1996. This legislation outlaws the possession, collection, duplication, transfer, or sale of trade secrets for purposes of using such secrets to benefit a foreign nation or any agent thereof.[70] In addition, the EEA grants the Department of Justice authority to enforce the law extraterritorially.[71] Finally, one of the most significant criminal statutes specifically applicable in the cyber context is the Computer Fraud and Abuse Act ("CFAA"), which prohibits intentionally causing damage—through the transmission of a computer code or program—to any computer connected to the Internet.[72] Al-

62 18 U.S.C. § 793(a)–(c) (2006).

63 *Id.* § 793(d)–(f).

64 *Id.* § 794.

65 *Id.* §§ 795, 797.

66 *Id.* § 796.

67 *Id.* § 798.

68 50 U.S.C. § 783(b) (2006).

69 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–1839).

70 18 U.S.C. § 1831.

71 *Id.* § 1837. For a discussion of the extraterritorial application of the EEA, see Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the TRIPS Agreement*, 78 N.Y.U. L. REV. 1475 (2003).

72 *See* 18 U.S.C. § 1030(a)(5)(A)(i).

though not directly related to espionage, the CFAA could presumably be relied upon for counterespionage purposes in the event of a cyber exploitation or attack.

As is true of U.S. laws regulating the offensive conduct of espionage, a common thread among these counterespionage statutes is their aim to punish acts that bear characteristics of theft and exploitation of state secrets. They address traditional forms of clandestine intelligence gathering rather than the features of influence and coercive force more readily associated with covert action. In general, the enforcement of these statutes is limited territorially inasmuch as the police power of the U.S. Government is so limited.

b. 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[73] or proscribing the coercion of political activity,[74] the federal criminal justice 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 U.S. borders (and external to the criminal justice system), such reactions must comply with the Constitution and applicable statutes, potentially including the covert-action reporting provisions. They are otherwise generally governed by international law, to which this discussion now turns.

C. International Law

1. Offensive Regulation

a. 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.[75] The UN Charter protects states from vio-

---

73 *See id.* §§ 2339A, 2339B.

74 *See, e.g.*, *id.* § 610.

75 *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,

lations of their territorial integrity and political independence involving the threat or use of force.[76] Scholars have raised concerns that some forms of intelligence gathering may transgress this right and violate the norm of peaceful cooperation among states, which is also fundamental to the UN Charter.[77] International law has very little to say, however, about the peacetime practice of espionage.[78] The fact that international law neither clearly condones nor explicitly proscribes the conduct[79] tends to support the conclusion that "[e]spionage is nothing but the violation of someone else's laws."[80]

---

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 Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 628 (2007) ("[M]ost experts today still agree that espionage remains part of the sovereign right of the nation-state.").

76 U.N. Charter art. 2, para. 4.

77 *See* Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (Roland J. Stanger ed., 1962); *see also* Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67 (1984) ("[E]spionage in peacetime is contrary to international 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."). Professor Delupis qualifies her view by explaining that espionage, although contrary to international law, is not an international *crime*—i.e., an offense indictable by international tribunal—"unless accompanied by other acts." *Id.* at 68. Even then, however, Professor Delupis claims that necessity or self-defense arguments could "nullify" the illegality of the conduct. *Id.* For an embodiment of the peaceful interstate cooperation norm, see U.N. Charter art. 1.

78 *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 in the event of capture."). As Professor Radsan has noted, "[t]hose words remain a fair assessment of the state of the literature today." Radsan, *supra* note 11, at 602; *see also* Chesterman, *supra* note 1, 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).

79 *See* Daniel B. Silver (updated & rev. by Frederick P. Hitz & J.E. Shreve Ariail), *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) (describing the "ambiguous state of espionage under international law").

80 *U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence, Part 5: Hearing Before the H. Select Comm. on Intelligence*, 94th Cong. 1767 (1975) (statement of Mitchell Rogovin, Special Counsel to the Director of Central Intelligence); *see also* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218–26 (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).

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.[81] With regard to nonintervention, "[t]he foundational rules of sovereignty . . . provide some guidance on what restrictions, if any, might be placed on different forms of intelligence gathering that do not rise to the level of an armed attack or violate other specific norms."[82] 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."[83] According to Professor Chesterman, this rule prohibits unauthorized entry into and use of territory,[84] although the content of these proscriptions remains ambiguous.[85]

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.[86] The Outer Space Treaty does not prohibit collection using orbiting satellites.[87] And indeed, despite expressions of concern and pragmatic

---

81 *See* Chesterman, *supra* note 1, at 1077.

82 *Id.* at 1081.

83 S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

84 Chesterman, *supra* note 1, at 1082.

85 Professor 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) (contesting "the mistaken assumption that domestic and international law significantly limit the transfer of captured enemy combatants").

86 United Nations Convention on the Law of the Sea arts. 3, 19(2)(c), *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397, *available at* http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf; *see also* Chesterman, *supra* note 1, at 1082–83.

87 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. II, *done* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205, *available at* http://www.oosa.unvienna.org/pdf/publications/STSPACE11E.pdf ("Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.").

responses to interception of electronic communications, nowhere in treaty law are such forms of signals intelligence explicitly prohibited.[88]

The international law of diplomatic and consular relations implicitly acknowledges the tradition of intelligence collection by foreign agents operating under diplomatic cover.[89] Some provisions of the Vienna Convention on Diplomatic Relations ("VCDR") constrain espionage activity.[90] For example, diplomats have obligations to respect the 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."[91]

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 Professor Chesterman observes, the Anti-Ballistic Missile Treaty and the SALT I Agreement both provide for "national technical means of verification" of treaty compliance.[92] 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."[93] 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.[94]

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 possi-

---

88 *See* Chesterman, *supra* note 1, at 1086–87; *see also* International Telecommunication Convention art. 22, *done* Oct. 25, 1973, 28 U.S.T. 2495, 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").

89 *See* Chesterman, *supra* note 1, at 1087–88.

90 *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." (footnotes omitted)).

91 Vienna Convention on Diplomatic Relations art. 41(1), (3), *done* Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95.

92 Chesterman, *supra* note 1, at 1090–91.

93 *Id.* at 1091. Professor 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. *See id.* at 1091–92.

94 *See id.* at 1093–98.

bility of lawful espionage.[95] 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.[96]

b. Covert Action

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."[97] The norm of nonintervention reflected in the UN Charter may, however, implicitly prohibit subversive actions by one state in the territory of another during peacetime.[98] But as Jeffrey Smith, former general counsel to the CIA, 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 le-

---

95 To be sure, the foregoing survey of the international legal architecture governing offensive espionage is not exhaustive. Of particular relevance to the context of espionage conducted via computer networks is the Convention on Cybercrime, which requires signatory nations to implement, through their domestic legal systems, "a common criminal policy aimed at the protection of society against cybercrime . . . by adopting appropriate legislation and fostering international co-operation." Council of Europe, Convention on Cybercrime, *done* Nov. 23, 2001, S. TREATY DOC. No. 108-11, C.E.T.S. No. 185. Broadly speaking, this treaty provides that signatory nations will adopt laws curbing (1) unauthorized access to computer systems, (2) unauthorized interception of private data communications via computer networks, (3) alteration or damage of computer data, (4) alteration or damage of computer system functioning, and (5) misappropriation of a password or device for commission of any of the four preceding offenses. *See id.* To date, forty-seven nations have signed the Convention, and thirty of them have ratified it (including the United States). *See Id.* What the Convention does not do is proscribe cyber espionage and attack as between nations (or nonstate actors). Instead, signing the Convention commits nations to the adoption of *domestic* laws and remedies relating to such activities. Thus, while the Convention may well be an important treaty, it bears only indirectly on the present discussion. (For example, this Article has already clarified that espionage entails the violation of another nation's laws. *See supra* note 80 and accompanying text.)

It is noteworthy that the Senate's view on ratification (in 2006) was that U.S. statutes already proscribe the conduct covered in the Convention. *See* 152 Cong. Rec. 17,072 (2006) (declaring that "current United States federal law fulfills the obligation of Chapter II of the Convention for the United States"). As this Article demonstrates, however, enforcing these domestic statutes against actors who carry out cyber exploitations and attacks against the United States is immensely problematic.

96 *See supra* note 80 and accompanying text.

97 Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L L. 687, 692 (2007).

98 *See id.*

gal . . . ."[99] Put simply, there is no bright-line rule regarding the legal status of covert actions: some may be lawful, others unlawful.[100]

The criteria for determining the lawfulness of covert actions are contestable. Professor 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 attempts to destabilize a government, or (4) it entails common crimes such as a breach of data protection laws.[101] On the other hand, Article 51 of the UN Charter states that "[n]othing in the present Charter shall impair the inherent right of . . . self-defense" in the event of an "armed attack."[102] Viewed against the backdrop of this inherent right, a given covert action in response to an attack or use of force may represent a lawful exercise of self-defense, 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.[103] More ambiguous still are cases in which a state that has not been victimized by armed attack exerts force that does not violate the territorial integrity or political independence of another state, uses force against a nonstate actor, or employs covert coercion that does not amount to a use of force.[104]

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

---

99 Smith, *supra* note 75, at 545.

100 *See* REISMAN & BAKER, *supra* note 35, at 9–10.

101 Fleck, *supra* note 97, at 692–93.

102 U.N. Charter art. 51.

103 *Id.* art. 2, para. 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, the decision of the International Court of Justice in *Nicaragua v. United States* may have limited the availability of such claims to cases of force used in response to an *armed attack*. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 103–04 (June 27). Here I omit discussion of the debate surrounding anticipatory self-defense.

104 For a discussion of the extensive debate surrounding the definitions of "force" and "armed attack" in Articles 2(4) and 51 of the UN Charter, see Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011).

> force; and [4] whether covert coercion was implemented only after plausibly less coercive measures were tried.[105]

They add that any covert action must comply with the requirements of international humanitarian law ("IHL"), such as proportionality and discrimination.[106] That view seems to comport with the conventional legal interpretation under which the U.S. Government gauges covert actions.[107] And while their multifactored test is not necessarily authoritative, Professors Reisman and Baker provide a helpful point of departure for the impending discussion concerning the cyber context.

2. Defensive Regulation

a. 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 international fora for punishing acts of espionage.[108] Although no convention exists 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.[109] The VCDR also grants absolute

---

105 REISMAN & BAKER, *supra* note 35, 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, 26–28 (1972). According to Professors 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 35, at 115.

106 REISMAN & BAKER, *supra* note 35, at 77. This Article use the terms "IHL" and "LOAC" interchangeably.

107 NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES § 4.2.1, at 194 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] ("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.").

108 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 77, at 67–68.

109 Chesterman, *supra* note 1, 1082 n.43 (citing 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." (internal quotation marks omitted)). The *Third Restatement of Foreign Relations Law* further expounds the residual authority to exercise extraterritorial jurisdiction:

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.[110] There would thus seem to be ample grounds under international law for states' efforts to defend against espionage by other states and nonstate actors, without prohibiting states from engaging in espionage themselves.

b. Covert Action

A state invoking the authority of international legal institutions 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.[111] By the very nature of covert actions, efforts at attribution will often be problematic.[112] As indicated in the following discussion, this problem becomes all the more vexing when the activity one attempts to attribute is network-based.

D. 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, although

---

> 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.

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. f (known as the "protective principle").

110 Vienna Convention on Diplomatic Relations art. 9(1), *done* Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95.

111 *See* Rep. of the Int'l Law Comm'n, 53d Sess., Apr. 23–June 1, July 2–Aug. 10, 2001, ¶ 76, art. 2, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001) (Draft Articles on the Responsibility of States for Internationally Wrongful Acts); *see also* JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT, AND COMMENTARIES 81–85 (2002).

112 Fleck, *supra* note 97, 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 tribunals in the *Nicaragua* and *Tadic* cases, respectively. *See id.* at 695–98; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 62–65 (June 27); Prosecutor v. Tadic, Case No. IT-94-1-A, Judgement, ¶¶ 98–145 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999), http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf.

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, but 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.[113]

The law thus conceptually places covert action in a category of coercion, use of force, and 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. Although this observation may seem mundane, it holds important consequences for the legal analysis of intelligence activities. The remainder of this Article explores the degree to which collection of intelligence using cyber networks frustrates the exploitation/coercion 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.

II. Unique Aspects of Cyber Networks

At least three characteristics 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. 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," Professor Susan Brenner and information analyst 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.

113 *See supra* notes 106–07 and accompanying text.

> 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.[114]

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,[115] 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.[116] Territorial limits on the exercise of police power may constrain the capacity of law enforcement agencies to deter espionage conducted from remote locations.[117]

2. Attribution Problem

A second unique characteristic of cyber activity is known as the *attribution problem*. The core of the problem is that, because cyber intrusions and attacks

> can be launched largely in secret, the identities of the actors carrying them out often cannot readily be determined. 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.[118]

In addition to identifying the responsible party, determining whether a given cyber intrusion was intentional or inadvertent is

---

114 Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 418 (2006) (footnote omitted).

115 "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 Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (July 8, 2005), http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

116 *See* Mindi McDowell, *Cyber Security Tip ST04-015: Understanding Denial-of-Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/cas/tips/ST04-015.html (last updated Nov. 4, 2009).

117 *See* discussion *supra* Part I.B.2.a; *see also* Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 24, 2010, at 21, 23 (reviewing RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010)).

118 Richard L. Kugler, *Deterrence of Cyber Attacks*, *in* CYBERPOWER AND NATIONAL SECURITY, *supra* note 5, at 309, 317 (noting also that "[t]he alleged but ambiguous Russian cyber attack on Estonia is another obvious example" of the attribution problem at work).

wrought with difficulty.[119] The attribution problem thus portends considerable difficulties for those seeking effective methods of deterrence against cyber intrusions.

3. Exploitation/Attack Quandary

A third distinctive aspect of cyber operations is the thorny issue of distinguishing cyber intrusions that constitute theft or exploitation from those that rise to the level of "armed attack" or "use of force." 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")[120] and *information war* ("cyber conflict at the nation-state level involving either direct military confrontation or indirect competition via disruption and deception").[121] I will refer to this problem as the exploitation/attack quandary ("EAQ").

Cyber attack can usefully be conceived of as "actions—perhaps taken 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 networks."[122] 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."[123] 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.

---

119 *See* Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 69 (2009).

120 Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY, *supra* note 5, at 437, 440.

121 *Id.* at 441. Ontologically, this bifurcation is likely something of an oversimplification. Professor Lachow, for example, suggests that at least three additional categories should be included: cyber crime, cyber terrorism, and "hacktivism." *See id.* at 438–41. However, in order to focus the inquiry on the narrow questions this Article seeks to address, the either/or distinction will be most useful.

122 NRC REPORT, *supra* note 107, § 1.4, at 19. The Stuxnet computer worm that reportedly caused the destruction of nearly twenty percent of Iran's nuclear centrifuges, thereby delaying the progress of the Iranian nuclear program, provides a useful example of cyber attack. *See* William J. Broad et al., *Israeli Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1.

123 NRC REPORT, *supra* note 107, § 1.4, at 20.

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,[124] international law remains ambiguous on the issue.[125] 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.

a. 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.[126] In such a scenario, the perpetrator of the intrusion could presumably act with the intention (or primary purpose) of collecting 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 instead, as a use of force or 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 armed attack (because 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

124 *See* Office of Gen. Counsel, Dep't of Def., *An Assessment of International Legal Issues in Information Operations* (2d ed. Nov. 1999), *reprinted in* 76 NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES app. at 483 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002), *available at* http://www.usnwc.edu/Research---Gaming/International-Law/RightsideLinks/Studies-Series/documents/Naval-War-College-vol-76.aspx.

125 *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041–42 (2007).

126 NRC REPORT, *supra* note 107, §§ 2.6.4.2, 2.2.3, at 154, 89.

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.*[127]

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 III, about the level of prudence the party launching the exploitation 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 Dan Geer has explained, one of the unique problems of cyber security is that "the original owner continu[es] to possess stolen data after the thief takes it."[128] This problem may further erode the distinction between cyber exploitation and cyber attack insofar as the distinction is grounded in a notion that attacks are tangibly destructive. In the information age, a nation's crown jewels need not be physically annihilated in order to be rendered ineffective. What is more, those jewels can be commandeered for use as a threat or weapon against that nation. And given this state of affairs, with our widespread dependence on computer networks—including for the

---

127 *Id.* § 2.1, at 81 (emphasis added).

128 Daniel E. Geer, Jr., *Cybersecurity and National Policy*, 1 HARV. NAT'L SECURITY J., Apr. 7, 2010, at 203, 204, http://www.harvardnsj.com/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf. .

functioning of military and intelligence systems—the United States may have more to lose than any other nation.[129]

b. 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, Director of the U.S. Cyber Consequences Unit, explains, three embedded characteristics of the United States' information-based economy leave us susceptible to targeted attacks.[130] 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.[131] 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 interferes with another, and so on.[132] Near monopolies, in which one or two companies provide virtually identical products or services to an entire industry, leave the economy vulnerable to *multiplier effects*, which emerge after an attack on business operations that supply an essential service or good to an entire industry that is dependent on that service or good for normal functioning.[133]

Aside from these economically oriented effects, "second-order effects" of cyber attacks may include "fear, loss of confidence in banking and communications systems, and a national awareness of vulnerability."[134] A particularly serious cyber attack, such as the "multiple denial-of-service attacks carried out against Estonia in April and May 2007," "could lead to even more enduring negative consequences than a limited military incursion."[135] And indeed, evidence suggests that

---

129 *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT, at xiii, 157 (2010).

130 *See* Scott Borg, *Economically Complex Cyberattacks*, IEEE SECURITY & PRIVACY, Nov.–Dec. 2005, at 64, 64.

131 *Id.*

132 *Id.* at 64–65.

133 *Id.* at 65.

134 Thomas C. Wingfield, *International Law and Information Operations*, *in* CYBERPOWER AND NATIONAL SECURITY, *supra* note 5, at 525.

135 *Id.*

even relatively limited and determinate cyber operations can spawn significant unintended consequences.[136]

The knock-on effects problem may exacerbate the EAQ. In the event that the cyber intrusion itself—even if engaged in for purposes of intelligence collection—is undertaken using an attack vector,[137] it may implicate some of the same concerns as those raised by what Borg calls "economically complex cyberattacks."[138] More research is needed to evaluate the degree to which cyber exploitations may generate the amplifying effects cited above as characteristic of cyber attacks. But it seems plausible that at least some cyber espionage operations will be based on platforms of cyber attack—for example, where an initial attack makes possible the follow-on theft of information for intelligence purposes. It may take time for the various consequences of such an intrusion to unfold, and as they do begin to appear, state actors may face severe difficulty in tracing data sets (e.g., 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 qual-

---

136 To take one example, in May 2010 it was reported that the U.S. military had used a cyber attack to dismantle an extremist website that was being jointly administered as an intelligence-gathering tool through a CIA-Saudi partnership. According to the report, the Pentagon operation "inadvertently disrupted more than 300 servers in Saudi Arabia, Germany and Texas," illustrating that in the cyber domain, "an attacker can never be sure than an action will affect only the intended target." Ellen Nakashima, *For Cyberwarriors, Murky Terrain: Pentagon's Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Policies*, WASH. POST., Mar. 19, 2010, at A1.

137 The range of typical information-warfare weapons contemplated by invocation of the term "attack vector" includes the following:

> *Trojan Horse*: a program remotely installed into the controlling switching centers of the Public Switched Network; *Trap Door*: a program used to gain unauthorized access into secured systems; *Logic bomb*: lies dormant and can be hidden within a Trojan Horse until a trigger condition causes it to activate and destroy the host computer's files; *Video-morphing*: makes broadcasts indistinguishable from normal transborder data flows; *Denial of service attack*: prevents networks from exchanging data; *Computer worm or virus*: travels from computer to computer across a hospitals [sic] network, damaging files; *Infoblockade*: blocks all electronic information from entering or leaving a state's borders; *Spamming*: floods military and civil email communications systems with frivolous messages, overloading servers and preventing field communications; *IP spoofing*: fabricates messages whereby an enemy masquerades as an authorized command authority.

Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L., Feb. 2010, at 22, 23 n.12 (citing Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 836–39 (2001)).

138 Borg, *supra* note 130, at 64.

ify 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[139]—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. Focusing on the EAQ, however, 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 an entirely 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 that discover foreign-based surveillance by way of electronic intercept, but states have likely structured policies that attempt 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.[140] Nonetheless, the difficulty of identifying one's 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 continue to develop increasingly robust capabilities for identifying cyber perpetrators through all-source intelligence and technological advancements.[141] Moreover, some commentators have argued that the scope of the attribution problem has been somewhat overstated.

---

139 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. *See, e.g.*, NRC REPORT, *supra* note 107, § 1.6, at 21; Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 187–89 (2006); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 251 (2009).

140 *See, e.g.*, Shackelford, *supra* note 139, at 233 (describing the "crucial issue of attribution" and declaring that "[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); Todd, *supra* note 119, at 67 (identifying attribution and espionage as "the most challenging aspects of cyberspace").

141 *See* Kugler, *supra* note 118, 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, July 3, 2009, at A1; Warwick Ashford, *US Works with ISP to Test Einstein 3 Cyber Security System*, COMPUTERWEEKLY.COM (Mar. 23, 2010, 3:56 PM) http://www.computerweekly.com/Articles/2010/03/23/240695/US-works-with-ISP-to-test-Einstein-3-cyber-security.htm.

As Franklin Kramer, former Assistant Secretary of Defense for International Security Affairs, 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."[142] 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.[143]

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

III. Implications of the EAQ

The difficulty of distinguishing between cyber espionage/exploitation and cyber warfare/attack entails a blurring of the legal and theoretical distinction between intelligence collection and covert action. A core practical implication of this conceptual breakdown is that executive branch lawyers in the information age face increasingly difficult judgment calls in determining which legal paradigms to turn to as policymakers initiate and respond to intrusive acts in cyberspace. If there is a normative implication to be drawn from this emerging reality (while bracketing the possibilities of legislative reform and negotiation of a treaty governing information operations), it may be 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 the descriptive conclusion to offensive uses of espionage and covert action, then turns 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.[144] Second, that absent an international conven-

142 Franklin D. Kramer, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, *in* Cyberpower and National Security, *supra* note 5, at 3, 16.

143 Kugler, *supra* note 118, at 317–18.

144 *See* NRC Report, *supra* note 107, § 4.3, at 198 (noting that, in light of the public information available regarding cyber exploitation of business and personal information as well as the

tion 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."[145]

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. In light of the EAQ and the often unpredictable consequences potentially attendant to cyber activities, however, a good number of cyber intrusions may blur the distinction between espionage and covert action. A policy of 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, would seem to be a judicious means of accounting for the new reality.

1. Domestic Regulation

As discussed in Part I, 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.[146] These relatively demanding procedures do not apply to, among other things, 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.

Department of Defense, "it would be highly surprising if the U.S. intelligence community did not know about and make use of cyberexploitation when appropriate or helpful").

145 *See supra* note 124 and accompanying text (noting that this is the Department of Defense's view); *see also* NRC REPORT, *supra* note 107, § 1.6, at 21 ("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.").

146 *See supra* notes 50–55 and accompanying text.

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 properly can 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[147]—this manifestation of the crown jewels problem would entail the very species of consequence that Congress sought to regulate by subjecting covert actions to careful oversight.[148] 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 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.

Applying the covert-action legal paradigm to more cyber espionage operations would comport with Congress's expressed concern about distinguishing covert action from collection based on the objective consequences of the activity. It would also align with the U.S. Government's current view of the distinction between attack and exploitation. Given that government lawyers generally look to the consequences of a cyber intrusion against the United States to determine whether that intrusion is an attack or an exploitation,[149] it would seem reasonable to judge our own actions with a symmetrically consequence-based approach. That is, even if the primary purpose of a proposed cyber operation is intelligence collection, if coercive or attack-level effects are foreseeable, then it may be necessary to vet that operation as if it were a cyber attack in order to maintain consistency with our defensive treatment of such operations. A related issue with which executive branch lawyers will need to wrestle is whether an agency can reasonably describe an action as having the primary purpose of collection when that agency is aware of the likelihood that

147 *See* S. REP. NO. 102-85, at 42 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 235.

148 *See supra* notes 56–58 and accompanying text.

149 *See supra* note 124 and accompanying text; *see also supra* note 139 and accompanying text.

covert-action-style consequences may well ensue from the proposed operation.

2. *International Law Model*

Many of the same concerns set forth above translate to the context of international law. Treating an increased number of cyber exploitations as covert actions would account for the fact that cyber exploitations may be more fittingly analyzed under the LOAC paradigm than a purely domestic law model. The CIA and other intelligence agencies already review all covert actions, whether or not they involve violent activities, for compliance with LOAC.[150] The same cannot be said about espionage activities. Given the general difficulty of distinguishing cyber exploitation from cyber attack, the choice to evaluate such operations *as if* they were cyber attacks—perhaps using Professors Reisman and Baker's four-pronged test for compliance with *jus ad bellum* and *jus in bello* discussed in Part I[151]—would seem a prudent check on the danger that activity intended as espionage could cross the line into unlawful warfare or use of force. The United States could be placed at risk of political or military backlash if its cyber-collection activities, conducted free of the high-level contingency planning and scrupulous oversight associated with covert action, created spillover effects or were interpreted as rising to the level of "armed attack" or "use of force" under international law.

It bears emphasizing that this discussion brackets many of the most complex questions involving the legal distinctions between armed attack, use of force, and coercion in the cyber domain. To be sure, the ongoing debate over such distinctions raises important questions whose bearing on determinations about the legality of cyber operations should not be understated.[152] My aim, however, is not to propose criteria for classifying various cyber operations in one or another of these conceptual categories.[153] It is instead to point out that, in contrast to laws governing espionage, there is room within the legal framework of covert action for all such means of influencing political, economic, or military conditions abroad.

---

150 *See supra* note 107 and accompanying text.

151 *See supra* notes 105–06 and accompanying text.

152 *See generally* Waxman, supra note 104.

153 This Article also does not attempt to tackle such questions as whether an activity that would otherwise be a covert action is undertaken with the intent to "prepare the battlefield" for anticipated hostilities. *See supra* note 53.

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 can be conducted[154] 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 and those with a traditional counterintelligence function[155] might seem tailor-made to establishing a broad program of cyber exploitation constituted as ordinary intelligence or counterintelligence activity.[156] Moreover, in passing the Intelligence Authorization Act of 1991, 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."[157] Hawkish types might argue that because 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 mission at a critical time. And more dovish observers might contend that lumping a whole slew of collection activities into the covert-action rubric will desensitize us to the need to ensure that covert actions are rare and dangerous policy tools, to be adopted only as measures of last resort.

---

154 *See* NRC REPORT, *supra* note 107, § 6.1.2, at 221 ("[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.").

155 *See supra* note 53 and accompanying text.

156 Support for this proposition can be found in the National Research Council report's suggestion that the intent of the intruder may be central to the distinction between cyber exploitation and cyber attack. *See* NRC REPORT, *supra* note 107, §§ 1.6, 7.2.2.1.5, at 22, 261 (noting that "the distinction between cyberattack and cyberexploitation may be very hard to draw from a technical standpoint, and may lie primarily in the intent of the user," and that "the question of intent is central to the targeted nation at the time [a] potentially hostile platform is detected"). As discussed above, however, the legislative history of the covert-action statute reflects Congress's desire that the definition of covert action "focus[ ] on the *objective features* of the activity, rather than on a formal relationship to foreign policy purposes, as the controlling test." S. REP. NO. 102-85, at 43 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 236 (emphasis added); *see also supra* text accompanying note 56. Given this context, it is not clear why the formalistically "primary purpose" of intelligence collection should make all the difference between espionage and covert action.

157 S. REP. NO. 102-85, at 42, *reprinted in* 1991 U.S.C.C.A.N. at 235.

These legitimate concerns must be addressed in any attempt to construct a coherent oversight framework for cyber operations. The impracticality of subjecting the entire scope of Title 50 network-based intelligence collection to covert-action oversight procedures is beyond dispute. It is surely infeasible 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 12,333[158] 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.[159] 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. So long as proper procedures are followed and agencies devote sufficient resources and personnel to the tasks of studying and explaining to policymakers the various modes of cyber exploitation, the risk of trivializing covert action under this approach is likely to be minimal. The interdepartmental exertion of energy and resources involved in clearing these activities through the chain of oversight may provide a check against political or moral anesthetization.

Even with the oversight procedures involved, a more sweeping categorization of various types of intrusion under the auspices of a single, ongoing covert action could less easily be said to hamper the United States' efforts to keep up with its adversaries in the cyber domain than a system requiring individualized approval. To the extent it does constrain the profusion of certain intelligence operations, the concerns outlined above suggest that such constraints may be called for. Put simply, a measure of self-imposed restraint in this context is justified, at least inasmuch as that restraint aids the efficient prevention of unanticipated negative fallout or blowback stemming from the nature of generative networks and layered vulnerabilities.

4. Drawing Lines

The preceding discussion has not addressed the significant line-drawing problem created by subjecting more cyber exploitations and

158 Exec. Order No. 12,333, § 3.1, 3 C.F.R. 200, 214 (1982).

159 There is precedent for broad presidential findings, reportedly including President George W. Bush's authorization for lethal action against high-value terrorism targets after 9/11. *See* Radsan, *supra* note 35, at 539–41.

collection operations to the covert-action paradigm. Defining the precise boundaries of which types of cyber exploitations should be classified as traditional counterintelligence or intelligence-collection activities, 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 Article. Nevertheless, the foregoing survey reveals potential guiding principles. For example, an appreciation of the crown jewels problem suggests that network-based intrusions employed to collect intelligence on particularly high-value targets—such as an adversary's nuclear command and control system—could properly be characterized and vetted as covert actions. The same conceptualization would apply to operations that are primarily designed to collect intelligence but include, say, the clandestine placement of a logic bomb for possible future detonation. It seems plausible enough that the boundaries alluded to above could be established within and across the executive branch as experience with various methods of cyber exploitation and attack grows.

B. Defensive Cyber Activities

Just as the outcomes of offensive use of computer networks 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. 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 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 acts 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.[160] In comparison, covert (cyber) action would seem a potentially effective form of response where 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, the United States could lawfully respond to a cyber

160 *See* discussion *supra* Part I.B.2.a.

attack or exploitation against it with a covert action if the covert action (1) promotes the policy objectives of the UN Charter, (2) adds to minimum world order, (3) is consistent with contingencies authorizing overt use of force, and (4) is implemented only after plausibly less coercive measures have been tried.[161] Treating more exploitations targeted against the United States as covert actions would place more of them in the conceptual 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 itself construed as a use of force against the United States.[162] The executive branch would need to assess whether less coercive measures are reasonably available and what constitutes an appropriate level of response in light of the legal requirement of consistency with the UN Charter. But that very Charter contemplates the sovereign right of self-defense.[163]

Article 51 provides specifically that nations must report any countermeasures taken in response to an "armed attack" to the UN Security Council.[164] Characterizing a cyber intrusion as a covert action, however, need not, and indeed often will not, equate to calling it an "armed attack."[165] As Professors Reisman and Baker explain, covert actions sometimes entail acts that constitute coercion or use of force but fall below the baseline of armed attack.[166] The important point here, again, is not to distinguish between armed attack, use of force, and coercion, but instead to observe that the legal framework of covert action—unlike the law of espionage—accommodates all of these concepts.

The National Research Council report observes that "[t]he issue of whether a nation may respond militarily without Security Council authorization if it is the target of a use of force short of an armed attack is less clear" than the issue of military response in the event of

---

161 *See supra* note 105 and accompanying text.

162 This example admittedly oversimplifies the range of issues at play in such circumstances, but it is offered to illustrate the broader conceptual point.

163 U.N. Charter art. 51; *see supra* note 102 and accompanying text.

164 U.N. Charter art. 51.

165 *See* NRC REPORT, *supra* note 107, § 1.8.3, at 33–34.

166 *See generally* REISMAN & BAKER, *supra* note 35, at 78–88.

an armed attack.[167] Covert action involving coercive and forceful conduct, however, is distinguishable from a military response (in armed attack) so long as its effects do not meet the armed-attack threshold. The need to ensure that certain forms of cyber espionage or other covert action employed in response to uses of force that fall short of armed attack do not themselves create the effects of an armed attack provides all the more reason to subject those responses to the stringent oversight requirements of covert action.

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 offensive and defensive capabilities to conduct effective counterintelligence. To the extent that more cyber exploitations against the United States are viewed 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.

Deterrence in the realm of cyber conflict is a profoundly complex and difficult exercise.[168] Technical defenses against specific forms of exploitation and attack are similarly difficult given the challenges of identifying and repairing vulnerabilities.[169] Professor Jack Goldsmith has observed that the "territorial limits on police power" and "very high threshold for military action abroad" amplify our vulnerability and the ease with which people outside one country can invade and disrupt "computer systems and all that they support inside another country."[170] Likewise noting that in this cyber game, "the contest between the offense and the defense is dreadfully mismatched, with the advantage strongly in the offensive corner,"[171] James Gosler has called 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

---

167 NRC REPORT, *supra* note 107, § 7.2.1.1, Box 7.1, at 244.

168 *See generally id.* § 9.1, at 302–05.

169 *See generally id.* § 2.2.2.1, at 83–86.

170 Goldsmith, *supra* note 117, at 23.

171 James R. Gosler, *The Digital Dimension*, *in* TRANSFORMING U.S. INTELLIGENCE 96, 96 (Jennifer E. Sims & Burton Gerber eds., 2005).

> and a tight coupling of our defensive and offensive elements.[172]

Echoing Gosler's position, intelligence officials have hinted at similar concerns regarding the need for proactivity and the limits of passive defense in the cyber context.[173]

Coupling defensive and offensive elements entails a much broader range of reforms to current practice than can be addressed in this space.[174] The point here is to suggest only that the offensive use of covert action as a protection 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.[175] While preserving domestic legal remedies for cases in which actors can be readily identified and prosecuted, a robust covert-action program may be a critical strategy of deterrence and counterintelligence until the utopian day when we might rely on the goodwill and self-restraint of states and nonstate actors to adhere to mutually agreed terms of international engagement absent an external enforcement structure.

CONCLUSION

The conventional distinction between espionage and covert action goes something like this: "Espionage seeks to know the world. . . . Covert action seeks to change the world."[176] This Article suggests that the use of cyber networks as a medium for espionage may cast doubt upon the continuing relevance of the conventional view. Lawyers and policymakers in the U.S. Government must begin to take seriously the reality that acts of cyber espionage undertaken with the intent to "know the world" have the potential to change the world in ways that are significant and sometimes difficult to predict. The "game change"

---

172 *Id.* at 103.

173 *See* NRC REPORT, *supra* note 107, § 4.3, at 199 (citing the February 2008 testimony of former DNI J. Michael McConnell before the Senate Select Committee on Intelligence).

174 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 173 (Jennifer E. Sims & Burton Gerber eds., 2009).

175 Presumably the judgment about whether any given intrusion is a covert action against the United States could be based on the same criteria that govern our own offensive categorization of such operations.

176 WEINER, *supra* note 34, at 11.

in the spy game is thus a story of conceptual obfuscation: between collection and covert action, exploitation and attack.

In seeking to lay bare the rough contours of this problem, the foregoing discussion has focused on how the EAQ might change the nature of espionage from a practical lawyering standpoint. The policy realignment tentatively suggested by this project is that the legal paradigm of covert action often may be the more appropriate framework of oversight for conceptualizing, initiating, and responding to clandestine acts of exploitation and attack in the cyber domain. This is partly a hedge on the crown jewels and knock-on effects problems, reflecting the unpredictability attendant to computer-network operations. But it also represents a measured attempt to preserve flexibility among offensive exploitation and attack alternatives. The difficulty of defense and deterrence in cyberspace renders the need for such flexibility palpable.

Further research is needed to better understand the extent to which consequences of the various modes of cyber intrusion can be predicted and controlled. It is plausible, however, that this Article's tentative conclusions would persist even if the attribution problem were to be largely mitigated 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 perfect confidence the degree to which it has been infiltrated when foreign states and nonstate actors launch computer-network attacks and exploitations, the judicious exercise of power through covert action promises to remain an indispensable feature of the nation's cyber arsenal.