# Topicality

## Security Cooperation

### Arms Sales

#### Arms Sales and Transfers require State Department involvement – that’s not Security cooperation

Congressional Research Service 22 [ The Congressional Research Service (CRS) serves as shared staff to congressional committees and Members of Congress. CRS experts assist at every stage of the legislative process — from the early considerations that precede bill drafting, through committee hearings and floor debate, to the oversight of enacted laws and various agency activities. “Arms Sales - Congressional Review Process” https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=2a6ef852-069e-49f2-854a-0ee1f994aec4&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A65P5-8D21-JC11-13S0-00000-00&pdcontentcomponentid=299219&pdteaserkey=sr1&pditab=allpods&ecomp=rz2yk&earg=sr1&prid=a549e521-5a95-41d1-94bc-a9e81fa9f6e2]//LP

Congressional Review Process Informal Notifications The Department of State (on behalf of the President) submits to the Senate Foreign Relations Committee and House Foreign Affairs Committee an informal notification of a prospective major arms sale 20 calendar days before the executive branch takes further formal action. An August 2020 State Department Office of Inspector General report explains that, in addition to the AECA formal notification process, 'the Department has by long-standing practice submitted a preliminary or informal notification of prospective major arms transfers in advance of their formal notification to the congressional committees of jurisdiction.'/3 The informal notification practice began with a February 18, 1976, letter from the Department of Defense making a commitment to give Congress these preliminary classified notifications./4 Beginning in 2012, the State Department implemented a new informal notification process, which the department calls a "tiered review," in which the relevant committees are notified between 20 and 40 calendar days before receiving formal notification, depending on the system and destination in question./5 \* \* \* 1 Originally titled The Foreign Military Sales Act. 2 For more information, see CRS Report R46337, Transfer of Defense Articles: Sale and Export of U.S.-Made Arms to Foreign Entities, by Nathan J. Lucas and Michael J. Vassalotti. 3 Review of the Department of State's Role in Arms Transfers to the Kingdom of Saudi Arabia and the United Arab Emirates, Department of State Office of Inspector General ISP-I-20-19, August 2020. 4 Letter of February 18, 1976 from Lt. Gen. H.M. Fish, USAF, Director, Defense Security Assistance Agency to Senator Hubert H. Humphrey, Senate Committee on Foreign Relations. 5 Prior to giving such notice, the State Department transmits to the committees any license applications for commercially licensed arms sales as soon as the department receives them. The State Department does not provide the same notice regarding government-to-government foreign military sales. \* \* \* During June 2017 testimony, Acting Assistant Secretary of State Tina Kaidanow described this process as a 'review period during which the Committees can ask questions or raise concerns prior to the Department of State initiating formal notification. The purpose is to provide Congress the opportunity to raise concerns, and have these concerns addressed, in a confidential process with the Administration, so that our bilateral relationship with the country in question is protected during this process.'/6 The State Department "generally will not formally notify an arms transfer if a member of Congress raises significant concerns by placing a hold during the informal review stage," the Inspector General report states, noting that "the Department is not precluded from proceeding with an arms transfer subject to a congressional hold."/7 Formal Notifications The AEA contains provisions for congressional review and disapproval of arms sales. The President may not proceed with a proposed FMS or DCS transaction if Congress adopts a joint resolution of disapproval within the statutory review periods described below. It is worth noting that a congressional recess or adjournment does not stop these review periods. Foreign Military Sales Section 36(b)(1) of the AECA requires the President formally to notify the Speaker of the House, as well as the Senate Foreign Relations Committee and House Foreign Affairs Committee, 30 calendar days before issuing a Letter of Offer and Acceptance (LOA) for an FMS-administered sale, enhancement, or upgrading of major defense equipment valued at $14 million or more; the sale, enhancement, or upgrading of defense articles or services valued at $50 million or more; or the sale, enhancement, or upgrading of design and construction services valued at $200 million or more./8 The Defense Security Cooperation Agency transmits the notifications to Congress./9 In the case of such sales to NATO member states, NATO, Japan, Australia, South Korea, Israel, or New Zealand, the President must formally notify Congress 15 calendar days before proceeding with the sale./10 \* \* \* 6 "Foreign Military Sales: Process and Policy," Statement Before the Subcommittee on Terrorism, Nonproliferation and Trade, House Foreign Affairs Committee, June 15, 2017. 7 Department of State Office of Inspector General, August 2020. 8 The Letter of Offer and Acceptance is the legal instrument used by the U.S. government for FMS transactions. (See CRS Report R46337, Transfer of Defense Articles: Sale and Export of U.S.-Made Arms to Foreign Entities.) The Foreign Assistance Act of 1974 (P.L. 93-559, 88 Stat. 1795) amended the Foreign Military Sales Act to add a $25 million dollar threshold for defense articles and services. The International Security Assistance and Arms Export Control Act of 1976 (P.L. 94-329, 90 Stat. 729) added major defense equipment with a $7 million threshold. The International Security and Development Cooperation Act of 1981 (P.L. 97-113, 95 Stat. 1519) changed the $7 million threshold to $14 million and the $25 million threshold to $50 million. The International Security and Development Cooperation Act of 1980 (P.L. 96-533, 94 Stat. 3131) added design and construction services with a $200 million threshold. 9 See E.O. 13637, "Administration of Reformed Export Controls," March 8, 2013. 10 For the Senate, these review periods appear to begin when the relevant Congressional notification notice is published in the Congressional Record.

### Actor

#### Security Cooperation on Cyber, AI, or Biotech requires Director of the Defense Technology Security Administration or Under Secretary of Defense for Acquisition, Technology, and Logistics action

DoD 16 [Pursuant to Title 10, United States Code, provisions in various National Defense Authorization Acts, and administrative practices relevant to certain security assistance authorities administered on behalf of the Department of State, this issuance establishes policy and assigns responsibilities for the administration of security cooperation to encourage and enable allied and partner nations to apply their military capabilities and capacities, consistent with U.S. strategy, priorities, and defense objectives “DoD Directive 5132.03: DOD POLICY AND RESPONSIBILITIES RELATING TO SECURITY COOPERATION” https://open.defense.gov/portals/23/Documents/foreignasst/DoDD\_513203\_on\_Security\_Cooperation.pdf]//LP

2.6. DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION (DTSA). Under the authority, direction, and control of the USD(P), the Director, DTSA: a. Develops DoD technology security policies related to foreign transfers of defense-related articles, services, and technologies. b. Builds technology security capabilities of U.S. allied and partner nations to increase interoperability and protect critical technology and information. c. In coordination with DoD Component heads, provides the security cooperation enterprise with information on allied and partner nations’ willingness and ability to protect sensitive U.S. information and technologies and how that may affect DoD security cooperation efforts. d. In coordination with Director, International Cooperation, Office of the USD(AT&L), prioritizes and pursues policies and defense agreements required to facilitate transfer of defenserelated articles, services, and technologies to allied and partner nations, including development of DoD anticipatory policies to support accelerated timelines to transfer such items to support security cooperation priorities. 2.7. USD(AT&L). The USD(AT&L): a. Establishes and maintains policies for the effective development of international acquisition, technology, and logistics programs, including international armaments cooperation (e.g., collaboration in science and technology; research, development, test, and evaluation; and acquisition, in-service, and logistics support (Acquisition and Cross-Servicing Agreements)), to support security cooperation goals. In coordination with the USD(P), leads the development of policies and procedures for the transfer of defense-related articles, services, and technologies to foreign countries, and co-chairs the Arms Transfer and Technology Release Senior Steering Group, to ensure such policies and procedures comply with national laws and regulations, including technology security and foreign disclosure requirements. c. In coordination with the USD(P) and the Department of State, identifies, prioritizes, and pursues defense acquisition-related agreements required to facilitate the cooperative development, acquisition, and transfer of defense-related articles, services, and technologies to allied and partner nations. d. Engages with industry to provide DoD priorities for allied and partner nation capability investments. e. Ensures that appropriate security cooperation activities are entered into G-TSCMIS to support planning and monitoring of security cooperation activities. f. Manages and administers those Title 10, United States Code, programs for which the USD(AT&L) has responsibility, consistent with security cooperation priorities. g. Coordinates on security cooperation policy guidance and theater campaign plans.

#### Any department can do Security Cooperation as long as they can justify it and the DoD agrees

US Code 18 [United States Code Annotated; last amended Aug. 13, 2018; Title 10: Armed Forces, Subtitle A: General Military Law, Part I: Organization and General Military Powers, “Security Cooperation,” Chapter 16 https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=36d1e120-61e0-4d13-85f2-d432af69ca97&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A8T8B-MS12-D6RV-H0B2-00000-00&pdcontentcomponentid=6362&pdteaserkey=sr20&pditab=allpods&ecomp=rz2yk&earg=sr20&prid=298b0942-ad47-415b-a269-8b26a8cf67ae]//LP

§ 385. Department of Defense support for other departments and agencies of the United States Government that advance Department of Defense security cooperation objectives

(a) Support authorized. Subject to subsection (c), the Secretary of Defense is authorized to support other departments and agencies of the United States Government for the purpose of implementing or supporting foreign assistance programs and activities described in subsection (b) that advance security cooperation objectives of the Department of Defense.

(b) Foreign assistance programs and activities. The foreign assistance programs and activities described in this subsection are foreign assistance programs and activities that—

(1) are necessary for the effectiveness of one or more programs of the Department of Defense relating to security cooperation conducted pursuant to an authority in this chapter; and

(2) cannot be carried out by the Department.

(c) Annual limitation on amount of support. The amount of support provided pursuant to subsection (a) in any fiscal year may not exceed $75,000,000.

(d) Notice and wait. If a determination is made to transfer funds in connection with the provision of support pursuant to subsection (a) for a program or activity, the transfer may not occur until—

(1) the Secretary and the head of the department or agency to receive the funds jointly submit to the congressional defense committees a notice on the transfer, which notice shall include—

(A) a detailed description of the purpose and estimated cost of such program or activity;

(B) a detailed description of the security cooperation objectives of the Department, including the theater campaign plan of the combatant command concerned, that will be advanced;

(C) a justification why such program or activity will advance such objectives;

(D) a justification why such program or activity cannot be carried out by the Department;

(E) an identification of any funds programmed or obligated by the department or agency other than the Department on such program or activity; and

(F) a timeline for the provision of such support; and

(2) a period of 30 days elapses after the date of the submittal of the notice pursuant to paragraph (1).

### Public Good

#### Security Cooperation must work towards overall public good

Van Ness 08 [Peter Van Ness is a Visiting Fellow, Department of International Relations, Research School of Pacific and Asian Studies, Australian National University https://ciaotest.cc.columbia.edu/wps/anu/0002776/f\_0002776\_1944.pdf]//LP

The future material gains from cooperation for all parties are potentially immense, especially with respect to investment, trade and technology transfer for the collaborative development and marketing of Russian energy resources. Meanwhile, the US and China would maintain their institutional ties in the region (for China, most importantly, the Shanghai Cooperation Organization and ASEAN+3; and for the US, its bilateral security ties with Japan, South Korea, Philippines, Thailand, Singapore and Australia), but in Northeast Asia, the most potentially volatile region in Asia, they would work together. Other countries in the Asia–Pacific may wonder about how such a new institution in which they do not directly participate will affect them. Seen in realist terms, those governments might worry that the security arrangement had been designed as a conspiracy against them. But cooperative security provides a different understanding. Multilateral security cooperation by a group of states in one region not only enhances their own security but also produces a public good of strategic stability for the larger community of nations. ASEAN has shown the way. The cooperative-security design in ASEAN has been built on a network of economic and political ties and strategic dialogue. If the Six Party Talks on Korea can now achieve as much as ASEAN already has achieved for its member-states (i.e., to make inter-state war among any of its members unthinkable), all countries in the region would benefit. Other countries in the region like Australia would not directly participate in the new institution, but they would benefit from the strategic stability and shared security achieved by the new, multilateral cooperative-security consortium—a public good.

## Artificial Intelligence

### AI v Autonomous

#### Artificial Intelligence and Autonomous systems are distinct

Sagramsingh 19 [Raine Sagramsingh is a recent graduate of the FAMU-FSU College of Engineering. She graduated summa cum laude with a Bachelor of Science in mechanical engineering. She was an active member of the Florida State University Center for Leadership and Social Change’s Service Scholar Program. Raine completed internships with the Air Force Research Lab and Northrop Grumman Aerospace Systems.https://wise-intern.org/wp-content/uploads/2019/04/Raine\_S\_-FinalPaper.pdf]//LP

The terms in which the international community discusses lethal autonomous weapons systems (LAWS) can at times be ambiguous as there is an absence of a common vocabulary and common understanding of the terms autonomy and artificial intelligence (AI). LAWS are weapons systems that apply lethal force independently, with freedom from human control. AI has many subfields including machine learning, data mining, speech recognition, and image processing. Policymakers frequently refer to any of the subfields of AI as AI. By grouping these various terms together under the umbrella of AI, the term is frequently misused by technical experts, policymakers, and the general public. As advances in technology lead to increased autonomy in systems, the terms AI and autonomy are frequently used together. Despite their relationship to each other, it is a mistake to use these terms interchangeably. Currently, the international discussion does not define the technical characteristics of LAWS, hindering the development of public policies, laws, and practices related to the use of autonomy and AI in weapons systems. To improve understanding of the technical characteristics of autonomy and AI in LAWS, this paper aims provides the following recommendations. Recommendation 1: Classify the level of autonomy and intelligence in current weapon systems. Members of the international discussion on LAWS should evaluate where current weapon systems fall on the spectrum of intelligence and autonomy and should consider which of those should or should not be a part of the continuing discussion. Recommendation 2: Limit the use of the term Artificial Intelligence. While potential exists for fully-autonomous intelligent weapon systems, they are not a current reality. Using the term AI to refer to machine learning, computer vision, natural language processing, and many other fields of study limits the development of public policy because there is no individual evaluation for their potential positive or negative impact on LAWS. Recommendation 4: Distinguish autonomous systems from autonomous intelligent agents. An autonomous system does not imply the use of AI, whereas autonomous intelligent agent does. These terms represent significantly different technologies that warrant separate discussion. Recommendation 5: Distinguish between semi- and fully-autonomous systems. To make progress developing public policies regarding LAWS, the discussion must distinguish semi-autonomous systems from fully-autonomous systems. Regulating the two technologies with the same set of policies ultimately will be unsuccessful.

#### AI has to problem solve not complete a task

Ball 20 [Inertial Sense has released the following article explaining the difference between autonomy and artificial intelligence (AI) as the two concepts relate to robotic systems. Inertial Sense is the developer of LUNA, an automated navigation software platform designed for robotics companies who want to make their existing fleet unmanned and automated. https://www.unmannedsystemstechnology.com/2020/11/artificial-intelligence-vs-autonomy-for-mobile-robotics/]//LP

Artificial Intelligence vs. Autonomy Artificial intelligence applications and autonomy are both valuable tools in the industrial environment. These technologies can be used independently or can work together to achieve the desired results. Here’s an easy way to breakdown the differences between the two: autonomous robotics = task completion and AI = problem-solving. Autonomous robotics systems are designed for use in predictable environments to complete tasks within a specific, usually pre-planned, environment. Sensors are of critical importance in providing robots with detailed and accurate information about their location within the domain. Autonomous robotics systems rely on these sensors to navigate their environments and to perform their tasks quickly and effectively. Autonomous devices and systems can be powered by conventional software or by AI systems that allow them to learn and adapt as they operate. Artificial intelligence is defined by Yale University as “building systems that can solve complex tasks in ways that would traditionally need human intelligence.” This typically involves machine learning technologies and the use of highly advanced sensors to collect information about the environment and to allow the system to react appropriately to external stimuli.

## Cybersecurity

### Cybersecurity Definitions

#### Cybersecurity involves market-based approaches

Ebrahim 20 [Tabrez Y. Ebrahim is an Associate Professor of Law, California Western School of Law; Visiting Associate Professor, University of California, San Diego; Ostrom Visiting Scholar (Program on Data Management and Information Governance) & Affiliate (Program on Cybersecurity and Internet Governance), Indiana University (Bloomington); Visiting Fellow, University of Nebraska (Lincoln): Nebraska Governance & Technology Center; Thomas Edison Innovation Fellow & Leonardo da Vinci Fellow, George Mason University Antonin Scalia Law School;ARTICLE: NATIONAL CYBERSECURITY INNOVATION. West Virginia Law Review, 123, 483. https://advance-lexis-com.proxy.lib.umich.edu/api/document?collection=analytical-materials&id=urn:contentItem:61X5-YX61-JX8W-M4YS-00000-00&context=1516831.]//LP

National cybersecurity involves tradeoffs with government intervention and market-based incentives for technological innovation, and theoretical reformulation of innovation mechanisms towards this lens is the subject of this Article. The patent system has been considered as supporting the establishment of a market of new technologies by providing incentives for invention, promoting the financing of innovation, and stimulating competition through exclusion. As such, while the patent system is a government-driven mechanism, the market foundation role of patents supports the market development of new technologies. [\*488] The parsing out of the government's need to provide national cybersecurity versus the private market in being able to provide national cybersecurity raises the question as to whether the patent system provides sufficient incentives for national cybersecurity innovation. A variety of innovation mechanisms could promote national cybersecurity innovation, and a comparison of the role of government and the market presents innovation policy considerations for society. Implicit in this analysis is that the patent system has some role in technological advancement for national cybersecurity. However, inventors and patent holders lack inadequate incentives from the patent system for national cybersecurity inventions, for which the guarantee of the reward is too small, the possibility of the reward is uncertain, or the transaction cost is too high. As a result, the patent system is inadequate to promote national cybersecurity innovation. Such limitations may push some national cybersecurity innovators towards trade secrecy, which presents a different set of problems, including whether and how they can help foster technological advancement to protect the critical infrastructure. The purpose of this Article is to assess how important the patent system is to national cybersecurity. If one unequivocal conclusion follows from this Article in addressing this tradeoff for achieving national cybersecurity, it is that patents may not be a good match when their disclosure is kept secret or when their interests can be taken by government, and technological innovation for critical infrastructure protection can be better oriented through prize funding or a better way to encourage public-private research and development ("R&D"). Innovation mechanisms for technological advancement present unique challenges for national cybersecurity, including market failure, government failure, and co-mingled public-private infrastructure elements. At a theoretical economic level, inventors and innovators will not make investments in national cybersecurity R&D and individuals hope to reap its benefits without contribution to its technology development - a conundrum that warrants government intervention. 17Link to the text of the note

#### Cybersecurity includes proactive measures

Craig et al 15 [Amanda N. Craig is a Senior Cybersecurity Strategist, Microsoft Corporation Scott J. Shackelford is an Assistant Professor of Business Law and Ethics, Indiana University; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University. Janine S. Hiller is a Professor of Business Law, Richard E. Sorensen Professor in Finance, Pamplin College of Business, Virginia Tech. Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. American Business Law Journal, 52, 721. https://advance-lexis-com.proxy.lib.umich.edu/api/document?collection=analytical-materials&id=urn:contentItem:5HRG-66D0-00CW-H0YN-00000-00&context=1516831]//LP

In the late 2000s and early 2010s, despite continued legal uncertainty in the United States and globally, debates about active cyber defense began to shift. More frequent cyber attacks increasing anxiety likely contributed to this change of perception; for instance, by 2010, more than forty percent of companies surveyed by Symantec reported that cybersecurity incidents topped their lists of concerns. As was mentioned above, one watershed moment was Operation Aurora, a sophisticated campaign using spear phishing attacks and at least one zero-day exploit exposed by Google in early 2010 The attacks were noteworthy for at least two reasons: the type of intellectual property that was stolen (including Google's source code--that is, its "crown jewels" 116Link to the text of the note) and the illustration of the extent to which state-sponsored attacks--or other highly organized and well-financed attackers--had begun targeting private firms. 117Link to the text of the note According to Dmitri Alperovitch, then-vice president of threat research at the antivirus firm McAfee, Operation Aurora "totally" changed the threat model, representing the first instance in which private firms (outside defense contractors) experienced "that level of sophisticated attack." 118Link to the text of the note Moreover, in Google's private investigation, the company gained access to a computer, located in Taiwan, "that it suspected of being the source of the [Aurora] attacks." 119Link to the text of the note When it saw evidence of attacks involving other U.S. companies, Google alerted and collaborated with U.S. intelligence and law enforcement agencies to trace ultimate responsibility for the [\*750] attacks back to mainland China. 120Link to the text of the note As such, Google may have "set a precedent of what is allowable" to defend against APTs--even as "one could imagine similar scenarios that could lead to civil or criminal charges." 121Link to the text of the note Operation Aurora did much to introduce the private sector to the concept of APTs, a term that, like "active defense," was borrowed from the military. 122Link to the text of the note In 2011, McAfee defined APTs as "sophisticated, covert attacks bent on surreptitiously stealing valuable data from targeted and unsuspecting companies" and claimed that such "targeted attacks are on the rise." 123Link to the text of the note Yet defining APTs may be a malleable and circumstantial exercise--and may even represent a politically or economically minded euphemism. In 2011, for example, the CEO of security firm HBGary said that the definition of an APT varies depending on "who you ask," and the terminology really only emerged because the U.S. Department of Defense and Air Force needed a "nice way" to refer to Chinese state-sponsored threats. 124Link to the text of the note Likewise, McAfee has argued that "the motive of the adversary … is the primary differentiator of an APT attack from a cybercriminal or hacktivist one" and agrees that APTs are targeted attacks "carried out under the sponsorship or direction of a nation-state [\*751] for something other than a pure financial/criminal reason or political protest." 125Link to the text of the note Yet this statement fails to appreciate that determining which motive dominates can be an even more daunting challenge than establishing attribution. Even though some industry experts have suggested that "APT hysteria" was overblown, and "some who [thought] that they [were] victims of APTs [were] really the victims of organized criminals, hacktivists, glorified script kiddies, and their own mistakes," evidence clearly demonstrates that malware has become more "customized," meaning anything from a simple repackaging of existing malware to "code written from the ground up for a specific attack." 126Link to the text of the note By 2013, more security experts claimed that sophisticated, targeted attacks posed the greatest information security "danger" for businesses that traditional defense technologies were "slowly losing relevance" because they were ineffective, 128Link to the text of the note and that companies were increasingly frustrated by attempting to protect themselves "with a purely defensive posture." 129]APTs are built to circumvent passive cyber defenses like firewalls and antivirus software. Private sector actors' self-reporting suggests that most advanced attacks go unnoticed for more than one year (and are often ultimately noticed by a third party); a reasonable conclusion is that APTs often circumvent purely defensive postures. In the early 2010s, continuing "massive cases of cyber exploitation," including GhostNet, Night Dragon, and Shady RAT, significantly harmed companies and advanced both media exposure and private [\*752] sector cybersecurity concerns, 131Link to the text of the note reinforcing the perception that APTs were the new norm. 132Link to the text of the note Moreover, APTs tipped cyber offense-and-defense asymmetry even further in the attackers' favor. Attackers already benefitted from the comparatively small risk of being caught and prosecuted; conversely, defenders already were forced to make significant investments and accept greater risks when deciding how to defend their networks. The rise of APTs enabled attackers to access greater resources and more advanced technologies (such as from a state sponsor or criminal organization) while private sector defenders continued to struggle to increase IT security budgets and employ less sophisticated technologies. According to security expert Keren Elazari in a report prepared for CrowdStrike, Simply put, the bad guys are gaining the upper hand. Cybercrime and corporate espionage attackers are persistent--and they only need to get in once… Advanced attackers are using previously unknown zero-day vulnerabilities and self-mutating, evasive, and polymorphic malware while detection rates of existing protection mechanisms are falling. Defenders are facing more malware and more sophistication. Attacks are as lucrative as ever for advanced and commonplace adversaries. Clearly, the time has come for a strategic shift of focus for cybersecurity. Active defense has emerged as the new security paradigm that can help defenders resolve the gap between detection and response and make life more difficult for attackers. In the face of escalating numbers and sophistication of cyber threats, and the imbalance between attackers and defenders, active defense emerged post-2010 as a practice that allows companies to increase the costs to adversaries attacking them---just as, in the physical world, allowing individuals to engage in self-defense increases the potential costs for would-be attackers, therefore possibly dissuading some attackers. However, even though active cyber defense is increasingly emerging as a [\*753] sensible or "logical" approach by which the private sector can shift a greater burden to attackers, what has been less clear is how the broader cybersecurity industry is evolving to support more proactive measures. The cybersecurity industry is an essential part of the evolution, as expertise and cybersecurity best practices reside in this space. Part II picks up this debate by couching it in the experience of dozens of cybersecurity companies and then focusing on four case studies before pivoting to consider some of the implications for businesses and policy makers in Part III.

#### Cybersecurity requires opinio juris and governmental processes

Shackelford et al 16 [Scott J. Shackelford is the Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution. Scott Russell is a Post-Graduate Fellow, Center for Applied Cybersecurity Research, Indiana University. Andreas Kuehn is the Zukerman Cybersecurity Predoctoral Fellow, Center for International Security and Cooperation, Stanford University; PhD Candidate School of Information Studies, Syracuse University. An earlier form of this article was published as Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector, in ETHICS AND POLICIES FOR CYBER WARFARE (Maria Rosaria Taddeo ed., 2016). We would like to thank Springer Nature for allowing the republication and expansion of this chapter as an article for the present volume. https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=e47f4f66-6c70-48c4-9602-c14f3a18937d&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5KG5-HR00-00SW-413V-00000-00&pdcontentcomponentid=237721&pdteaserkey=sr4&pditab=allpods&ecomp=rz2yk&earg=sr4&prid=94d3703c-3bc6-4a1c-8516-5ccfa8a69fd6]//LP

A. An Introduction to Customary International Cybersecurity Law One precedent informing customary international cybersecurity law was articulated by the ICJ in the Nicaragua v. United States case (Nicaragua), which involved a dispute over the United States' involvement with the Contra rebellion in Nicaragua. 11Link to the text of the note In Nicaragua, the ICJ held that customary international obligations would arise from the consistent, widespread practice of States engaging in specific acts or omissions, performed out of a sense of obligation that such acts or omissions were required by international law (opinio juris). The combination of opinio juris and State practice performed by a significant number of States and without the express disavowal of a significant number of other States, gives rise to international obligations under customary international law. The underlying rationale is that this combination reflects a consensus in the international community that the actions taken represent an international obligation. Despite Nicaragua's clear articulation of the rule, in practice, the development of customary international law presents a temporal dilemma. For a State to engage in actions out of a sense of legal duty, this decision presupposes the existence of such a duty, and therefore the prior existence of customary international law on a certain issue. 14Link to the text of the note To help resolve this dilemma, Professor Frederic Kirgis argued for what he calls a "sliding scale" approach. 15Link to the text of the note Professor Kirgis argues State practice and opinio juris need to be understood on a spectrum, wherein the requirement for opinio juris increases as the evidence of State practice decreases. Rather than [\*6] impose strict requirements for both State practice and opinio juris, the sliding scale approach argues that a strong history of State practice can give rise to international obligations absent opinio juris. 16Link to the text of the note Likewise, compelling opinio juris could give rise to international obligations with little evidence of State practice. 17Link to the text of the note The sliding scale approach may prove particularly important in the cybersecurity realm as these novel technologies have developed too rapidly for evidence of widespread State practice to emerge, yet compelling opinio juris may still form the basis for international obligations. Proving opinio juris, however, is a difficult task, especially in the cyber context. The temporal dilemma makes pointing to existing rules challenging, so the preferred method is to identify broad principles that enjoy widespread international agreement, which the ICJ suggests may be evidenced by treaties. 18Link to the text of the note Indeed, most courts rely on treaties to identify opinio juris, often exclusively so. 19Link to the text of the note Yet in the cyber realm, treaties have largely focused on implementing domestic cybercrime laws and have done relatively little to address cybersecurity standards, leaving such decisions to the private sector and standards bodies such as the NIST Framework, discussed below. 20Link to the text of the note So using cybercrime as an example, international agreements like the Budapest Convention, the African Union Convention on Cybersecurity and Data Protection, and the various Association of Southeast Asian Nations working groups on cybercrime all could serve as opinio juris that States have an obligation to enact and enforce cybercrime laws within their territories and to cooperate to prosecute and extradite cybercriminals. Even though these agreements often lack binding language, they nonetheless suggest a growing international consensus that the establishment of domestic cybercrime laws is an international obligation. 21Link to the text of the note Similarly, the Organization of American States has also encouraged Member States to join the Budapest Convention and to increase regional cooperation to mitigate cybercrime, whereas a nonbinding U.N. General Assembly Resolution calls on States to "eliminate safe havens" for cybercriminals. 22Link to the text of the note Declarations like [\*7] these, although non-binding, serve as further evidence of international consensus regarding cybercrime. While it is unlikely that a non-signatory State would be bound to the specific terms of a treaty to which it did not sign--particularly in the short term--that treaty may still serve to identify broad principles that form opinio juris and thereby can build a foundation for international obligations. The search for cybersecurity opinio juris is further complicated by the multifaceted cyber threat comprising cybercrime, espionage, terrorism, and war. While the classification of State cyber-activities is a well-known problem, 23Link to the text of the note the fact that these activities are so widespread suggests a lack of opinio juris against aggressive State cyber-activity below the armed-attack threshold. The ambiguity surrounding State cyber-activities is further reinforced by discussions of the international law relating to espionage, which is largely unregulated outside the law of war context. 24Link to the text of the note Similarly, domestic cybersecurity practices are highly variable and can involve the surreptitious installation of malware--as alleged of Chinese telecommunications providers and the National Security Agency (NSA) alike--discussed further below. 25Link to the text of the note Given the relative lack of multilateral progress, claiming a widespread consensus for an underlying cybersecurity norm is challenging: a situation that can only be marginally mitigated by investigating related ICJ jurisprudence on the subject. B. ICJ Jurisprudence as It Relates to Cybersecurity Due Diligence Although the ICJ has never directly addressed cybersecurity due diligence requirements, its cases discussing due diligence generally can serve as broad guideposts to infer cyber-specific applications. It is worth noting that these cases all arose prior to the proliferation of cyber attacks, but some of the principles that underlay the cases, including Corfu Channel, Trail Smelter, and Nicaragua, may still have some applicability. 26Link to the text of the note Before reviewing these cases though, it is first important to define "cybersecurity due diligence." In the transactional context, this term has [\*8] been defined as '"the review of the governance, processes and controls that are used to secure information assets."' 27Link to the text of the note The concept as it is used in this Article builds from this definition and may be understood as the customary national and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and effective governance mechanisms so as to promote cyber peace through enhancing the security of computers, networks, and Information and Communications Technology (ICT) infrastructure. Cybersecurity due diligence obligations may exist between States, between non-State actors (for example, private corporations, end-users), and between State and non-State actors. Applicable instruments include technical standards, legal requirements born from treaty or custom, as well as national policies and private-sector industry norms, discussed below. 28Link to the text of the note We will proceed by highlighting three international obligations identified by the ICJ: the duty to warn, the "no harm" principle, and non-intervention, which we will use to infer cyber-specific applications and identify potential problems. We will then go on to address the law governing countermeasures for when an international obligation is violated, address its applicability to cyber-operations, and consider the implications for cyber due diligence.