The Norm Against Economic Espionage for the Benefit of Private Firms:

Some Reflections about Intelligence Culture

Samuel J. Rascoff

Early Draft – Please do not Cite or Circulate

June 18, 2015

Traditional separation of powers contemplates the allocation of official authority between constitutionally created arms of government. Recent scholarship extends the discussion to the administrative state.[1] But rarely has the concept been employed to consider the relationship between the market and the state. And yet, some of the most dynamic and important issues surrounding contemporary national security law and policy implicate precisely this boundary. In this Essay, I aim to throw light on the complex interdependencies between the market and the national security state in light of evolving technologies.

My more particular focus is on the meaning and functions of a norm that has been around in national security law and policy in one shape or another for at least forty years, but has enjoyed something of a renaissance in the last 18 months in the post-Snowden era: the prohibition against intelligence collection for the sake of the enrichment of American businesses (what I refer to as the "norm"). This self-imposed constraint[2] on the national security executive has enjoyed relatively scant attention within the legal academy – a series of blog posts by Jack Goldsmith[3] remain the most important recent contributions to our understanding of its contours. But the norm has something important to teach about the culture of the American intelligence community and its relationship to the rule of law, or so I contend in this Essay.

My central argument is that Goldsmith's realist account of the norm, while capturing something significant about the present moment, does not adequately explain its origins, or the norm's staying power across decades. It also fails to account for the norm's peculiar purchase within the intelligence community, as opposed to other quarters of the national security state (or, for that matter, the balance of the "ordinary" state). To complement Goldsmith's realism, I offer a genealogy of the norm and an account of its durability rooted in the organizational culture of American intelligence and the self-conception of American intelligence professionals. In particular, I emphasize the norm's embodiment of the reluctance of intelligence professionals to subordinate their efforts to the bottom lines of profit-seeking corporations.[4] This is, I contend, an outgrowth of the American intelligence community's complicated outlook on the market, which historically conjoined a sense of superiority to quotidian economic affairs with a laissez-faire sensibility.

My core claim generates potentially policy-relevant insights. Most significant, the intelligence community's relationship to the rule of law emerges as more complicated (and perhaps also more promising) than is sometimes imagined. Law and law-like institutions can emerge organically from within the intelligence community; they need not arrive as transplants from another domain, enforced by institutional outsiders,

---

[1] See Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUMBIA L. REV. 515 (2015).
[2] See generally Nathan Sales, *Self Restraint and National Security*, 6 J. NAT'L SEC. L. & POL'Y 227 (2012).
[3] See Jack Goldsmith, *The Precise (and Narrow) Limits on U.S. Economic Espionage*, LAWFARE (March 23, 2015), http://www.lawfareblog.com/precise-and-narrow-limits-us-economic-espionage; *Reflections on U.S. Economic Espionage, Post-Snowden*, LAWFARE (Dec. 10, 2013) http://www.lawfareblog.com/reflections-us-economic-espionage-post-snowden.
[4] For an example of an ethnographic approach to the intelligence community, see ROB JOHNSTON, ANALYTIC CULTURE IN THE U.S. INTELLIGENCE COMMUNITY: AN ETHNOGRAPHIC STUDY (2005).

calculated to rein in an otherwise lawless enterprise. To be certain, the norm at question is modest in its ambition and practical application, especially in view of the ever-increasing levels of public-private collaboration throughout the national security state, prompted nowadays by the imperatives of cybersecurity. And as recent scholarship has highlighted, the intelligence community is capable of being punctilious about compliance with certain rules while paying insufficient attention to others.[5] But the story of the norm nevertheless complicates our understanding of how law emerges and functions within the national security state.

In Part II, I offer a brief genealogy of the norm and its evolution, before offering an analytic account of norm as it currently stands (including the considerable exceptions that it admits). In Part III, I offer some potential theoretical justifications for the norm, pointing out the limitations of each, including Goldsmith's realist account. In Part IV, I propose a cultural-organizational account of the norm's origins and durability, and then extrapolate from this insight to larger potential implications for the project of intelligence governance and for national security law more broadly. In Part V, I consider the limitations of the cultural account, taking stock of the strategic pressures that are currently arrayed against it, most notably the ever-greater levels of public-private collaboration demanded by cyber-security.

II.

Although PPD-28 represents its first appearance in a public document that enjoys the force of law,[6] the norm against economic espionage for the benefit of private firms is, in fact, not new. It dates back at least to the 1970s, a period of intense turmoil and change in the intelligence community. During the Nixon Administration, the President's Foreign Intelligence Advisory Board ("PFIAB") took up the question in the context of potential responses to the emergence of Japanese auto manufacturing and the threat that it posed to Detroit. Gerard P. Burke, who headed the PFIAB, recalled that the board took up the matter of the limits of economic espionage and "discussed it ad nauseam. We thought U.S. companies needed [support], but we didn't think it should be provided by the U.S. government. There were obvious conflicts of interest."[7] As Burke later reported of the Board's conclusion, "we said that while American companies need information of a tactical nature that would give them an edge when competing in the world marketplace, we did not believe that it was appropriate that the U.S. Government should provide that intelligence; the user companies should acquire it themselves."[8] President Carter's CIA Director Admiral Stansfield Turner strongly considered

---

[5] See Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARVARD NATIONAL SECURITY JOURNAL 112 (2015).

[6] According to Presidential Policy Directive 28, the White House's signature statement on intelligence reform after Snowden, "[t]he collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."

[7] JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 7 (1997). Turner apparently retained his belief even after leaving government. *See* Amy Borrus, *Should the CIA Start Spying for Corporate America?,* Business Week, Oct. 14, 1992, at 96 (quoting him to the effect that "We steal secrets for our military preparedness. I don't see why we shouldn't to stay economically competitive.").

[8] The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings before the Subcomm. on Economic and Commercial Law of the H. Comm. on the Judiciary, 102d Cong. 18 (1992) (response of Gerard S. Burke, intelligence expert consultant).

abandoning the norm, arguing "if [the economy] isn't a national security matter, then what is!?"[9] But faced with strong opposition of his senior staff, Turner relented.[10]

The issue next came to a head (and generated some public and scholarly attention[11]) in the aftermath of the Cold War. As former US Secretary of State Warren Christopher put it: "In the post-Cold War world, our national security is inseparable from our economic security."[12] Under conditions where certain legislators regarded the CIA as of limited value,[13] a debate emerged about how to deploy the intelligence community in the new strategic environment. As Congressman Dan Glickman (later to become Chairman of the House Intelligence Committee) put it, "America is much more at risk today by our industrial base being withered away than it is probably by the former Russian empire, and it is important that this country become lean and mean in fighting the economic threats of the rest of the world, particularly when our companies may be the targets of competitors who would think nothing of stealing secrets in a surreptitious way."[14]

In this environment, the George H.W. Bush administration released a strategy document that recognized the changing intelligence landscape and that openly considered "[w]hat kinds of economic intelligence . . . we need?"[15] But on the question of the norm, the CIA held firm: Director of Central Intelligence Robert Gates emphasized that "the CIA does not, and will not, engage in commercial espionage. We do not penetrate foreign companies for the purpose of collecting business information of interest to U.S. corporations. In our view, it is the role of U.S. business to size up foreign competitors' trade secrets, market strategies, and bid proposals. But we do operate overseas to monitor foreign government sponsored targeting of American businesses."[16]

The Clinton Administration undertook its own review of the prospects of economic espionage. Run by then-NSC Senior Director for Intelligence George Tenet, "a key consideration in this review was the role that the Intelligence community should play regarding foreign competitors of American business."[17] In 1993, following the review, CIA Director James Woolsey declared the administration's opposition to "spying on foreign corporations for the benefit of domestic businesses."[18] Two years later, a bipartisan commission reviewing the issue reached the same bottom line. Created by the Intelligence Authorization Act for Fiscal Year 1995, the Commission on the Roles and Capabilities of the United States Intelligence Community reviewed the role of the intelligence community in the "post-cold war global environment" and reported its

---

[9]

[10] Michael T. Clark, Comment, *Economic Espionage: The Role of the United States intelligence Community*, 3 J. INT'L LEGAL STUD. 253, 264 (1997).

[11] Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 Law & Pol'y Int'l Bus. 459, 459-60 (1994-1995); Mark Burton, *Government Spying for Commercial Gain,* 37 Stud. in Intelligence 18 (1994), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/unclass1994.pdf.

[12] Warren Christopher, *The Strategic Priorities of American Foreign Policy*, U.S. DEPARTMENT OF STATE DISPATCH, November 4, 1993, p. 2.

[13] See Daniel Patrick Moynihan

[14] The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings before the Subcomm. on Economic and Commercial Law of the H. Comm. on the Judiciary, 102d Cong. 4-5 (1992) (statement of Rep. Glickman).

[15] George H.W. Bush, National Security Review 29 at 2 (Nov. 15, 1991), *available at* http://fas.org/irp/offdocs/nsr/nsr29.pdf

[16] The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings before the Subcomm. on Economic and Commercial Law of the H. Comm. on the Judiciary, 102d Cong. 53 (1992) (statement of then-CIA Director Robert Gates).

[17] Evans, *supra* note, at 353-54.

[18] *Id.* at 356.

findings in *Preparing for the 21 Century an Appraisal of U.S. Intelligence*, which was released on March 1, 1996. The Commission concluded that "the intelligence community's activities in the area of economic intelligence should continue, but that it should have a limited role . . . . The Commission made it clear that the role of the intelligence community has not been, and should never be, for the benefit of private firms. The report states that "the role of the Intelligence Community is to provide support to the Government, not to the private sector."[19]

Of late, the norm has re-emerged as an issue in the context of post-Snowden discussions of the appropriate metes and bounds of U.S. surveillance and cyber-security initiatives. DNI Clapper underscored its ongoing importance to the intelligence community, and it was ultimately embodied in PPD-28. Prompting this renewed interest in the norm is a sense that diplomatic and businesses audiences at home but especially overseas want assurances that the U.S. is not employing its formidable electronic surveillance and cyber capacities to give American businesses a leg up in the global marketplace, and more generally that the American intelligence community is, in some respects, more constrained that foreign counterparts. (Conceived up as a source of reassurance to the American technology and telecommunications firms whose businesses overseas were disrupted by the Snowden documents, the norm can be seen as similar in spirit to the recently announced policy that the intelligence community will not employ vaccination programs in operational settings, so as not to cast a shadow on critically important public health functions.[20]) Whether the target audiences believe the American story is another matter; in the aftermath of Snowden, the German Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz – BfV*)[21] investigated whether or not the United States as involved in economic espionage against German business.[22]

It is worth considering a number aspects pertaining to the status and scope of the norm. First, until the recent PPD, it is not clear in what form – was it law? or internal regulation? – the norm was embodied. There are suggestions in the historical record that the norm was more a matter of CIA policy than law. For example, former CIA Director Bob Gates recently expressed the view that he frequently attempted to share the information with the Commerce Department. "I never could get one of [the five of six Commerce Secretaries with whom Gates interacted] interested in being the facilitator of getting that kind of CIA

---

[19] Clark, *supra* note, at 256-57.

[20] *How the CIA's Fake Vaccination Campaign Endangers Us All*, SCIENTIFIC AMERICAN (April 16, 2013). In http://www.scientificamerican.com/article/how-cia-fake-vaccination-campaign-endangers-us-all. The CIA responded by instituting a policy change, committing that "the Agency will make no operational use of vaccination programs, which includes vaccination workers." The letter also said the agency "will not seek to obtain or exploit DNA or other genetic material acquired through such programs." See Lena Sun, *CIA: No More Vaccination Campaigns in Spy Operations* WASH. POST (May 19, 2014).

[21] Official website at http://www.verfassungsschutz.de/ (partially available in English at http://www.verfassungsschutz.de/en/index-en.html) (last visited April 6, 2015). It considers economic espionage by foreign states a serious threat to the German economy. See economic security gateway of the BfV, partially available in English at http://www.verfassungsschutz.de/en/fields-of-work/economic-security, complete version in German at http://www.verfassungsschutz.de/de/arbeitsfelder/af-wirtschaftsschutz (last visited April 6, 2015).

[22] It concluded that it could find no credible evidence to support that claim. Findings confirmed by the official statement of the German Government of August 5, 2014, Concerning Intelligence Attacks and Espionage on German Enterprises, p. 4, available online at http://dipbt.bundestag.de/dip21/btd/18/022/1802281.pdf (nothing, however, that the BfV investigation into alleged U.S. based economic espionage will continue), reported by Die Welt, online sources (November 8, 2014), available at http://www.welt.de/print/welt_kompakt/print_wirtschaft/article131087264/Spaehangriffe-auf-deutsche-Firmen.html (both last visited April 6, 2015).

information to American companies. So this is something we don't do."[23] It would be hard to imagine Gates boasting about having tried to violate intelligence law. Even now that the norm is clearly embodied in law, it the President may potentially waive or amend. For example, the CIA in 1977 adopted an internal regulation to the effect it would not use missionaries or journalists to supply cover for the agency's operatives. But in rare circumstances, the Agency had the authority to waive that self-imposed constraint and did so.[24]

Second, whereas PPD-28 covers only the collection of signals intelligence, the norm is widely understood to cover the entire intelligence community. As Director of National Intelligence Clapper put it in a post-Snowden clarification of the metes and bounds of American economic intelligence gathering, "[w]hat we do not do . . . . is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line."[25] Although there is some suggestion that the norm bound (or binds) agencies outside the intelligence community,[26] it is not clear what, precisely, that may have meant or currently mean. And in any event there is also evidence pointing in the other direction. As Gates put it, "we maintain close liaison with other U.S. Government agencies. If we come across information that does not fall within our purview, we pass it to the appropriate department."[27]

Third, the norm is a distinctly American one. As Gates recently explained, "It's hard for people to believe this. You'll have to take my word for it. We are nearly alone in the world in not using our intelligence services for competitive advantage for our businesses."[28] He went on to say that "[t]he Chinese probably have the most pervasive system of collecting against us of any country, but I think it's important to remember they're not alone."[29] Indeed, the secondary literature in the area frequently identifies France as a leading practitioner of economic espionage,[30] something of which the French make no secret.[31]

Concerning the scope of the norm, a number of (potentially very significant) exceptions have always characterized this area. First, the norm focuses on offensive (or "positive") intelligence gathering. In other words, the norm has meant (and apparently continues to mean) that officials are not authorized to gather intelligence for the benefit of private firms. Intelligence agents may, however, gather and share information with firms about threats to their business. In other words, the norm has always been (and ostensibly

---

[23] Philip Ewing, *Gates: French Cyber Spies Stealing U.S. Technology*, Politico (May 22, 2014, 6:11 PM), http://www.politico.com/story/2014/05/france-intellectual-property-theft-107020.html.
[24] Walter Pincus, *CIA Official Reveals Agency's Use Of Journalists in Secret Operations*, WASH. POST (Feb. 16, 1996).
[25] http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage
[26] Clyde Prestowitz, *Got Intel, Uncle Sam? Share it with U.S. Companies*, L.A. Times (May 25, 2014, 4:00 PM), http://www.latimes.com/opinion/op-ed/la-oe-prestowitz-china-hacking-20140526-story.html.
[27] The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings before the Subcomm. on Economic and Commercial Law of the H. Comm. on the Judiciary, 102d Cong. 54 (1992) (statement of then-CIA Director Robert Gates).
[28] Philip Ewing, *Gates: French Cyber Spies Stealing U.S. Technology*, POLITICO (May 22, 2014, 6:11 PM), http://www.politico.com/story/2014/05/france-intellectual-property-theft-107020.html.
[29] Id.
[30] HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING (Cambridge University Press, 2005).
[31] This practice dates back to 1946, see Didier Lucas, *1994-2014: quelle organization de l'intelligence économique d'entreprise en France?*, 70 GÉOÉCONOMIE 147 (2014); see also the official statement by the French Government of May 29, 2013, at http://www.elysee.fr/conseils-des-ministres/article/compte-rendu-du-conseil-des-ministres-du-29-mai-201/ (last visited on April 4, 2015), stating (in relevant part) that "engaging in economic intelligence means to collect, analyze, disseminate and protect strategic economic information . . . for the benefit of all economic actors (companies, research institutions, ministries and regions)."

continues to be) fully compatible with robust information sharing in cases of perceived economic downside to businesses, but not in connection with providing firms with economic upside. This is especially noteworthy in an era of pervasive cyber-security threats to businesses.

Second, the norm appears to include a carve-out where the information being shared pertains to any alleged involvement of foreign officials in a business matter, including but not limited to cases of bribery. As a footnote in the recent Presidential Policy Directive explains, "certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage."[32] Assume that French officials are advocating for a French manufacturer to win a contract in Germany against a rival American bid. According to the way that the norm is typically described, the involvement of French officials would permit American intelligence officials to fall within an exception and to alert the American firm of the official involvement.

Third, and perhaps most significant, the norm is frequently described as preventing American officials from gathering information for the purpose of enriching private firms. In other words, the norm appears to be compatible with a strategy that, for example, regards the enrichment of certain firms under certain conditions as enhancing national security. As long as the purpose of the intelligence sharing is couched in national security terms, the fact that a firm or an industry may benefit is apparently alright.[33] As David Sanger explained, "the government does not deny it routinely spies to advance American economic advantage, which is part of its broad definition of how it protects American national security. In short, the officials say, while the N.S.A. cannot spy on Airbus and give the results to Boeing, it is free to spy on European or Asian trade negotiators and use the results to help American trade officials — and, by extension, the American industries and workers they are trying to bolster."[34]

III.

What theory best accounts for the norm? A number have been offered. Frequently summoned is the explanation that the norm is necessary to avoid a practical puzzle of how to distribute economically beneficial information to American firms in competitive industries.[35] The norm, on this account, is motivated by the desire to prevent the government from facing the dilemma of creating competitive advantages within industry sectors, or sharing intelligence with an entire sector. But while this practical dilemma captures something true about the complexity of transferring knowledge from a monopolist (the intelligence community) to a competitive market, it seems inadequate to justify the emergence and durability of the norm.

---

[32] Directive on Signals Intelligence, ## Weekly Comp. Pres. Doc. 3 (Jan. 17, 2014), *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201400031/pdf/DCPD-201400031.pdf.

[33] See Burton at 14 ("There are gray areas in which businessmen may provide information to their country's intelligence service regarding foreign competitors or clients. Conversely, defense contractors or other national security-related businesses may be provided government intelligence data because they are required for a special project, such as the development of a weapon system. But in both of these cases, intelligence is being used for national security purposes and not for commercial gain. In the case of a defense contractor, the contract and, hence, profit has already been obtained. The intelligence information is simply being used to improve the characteristics of a given system being produced by the contractor.").

[34] David E. Sanger, *Fine Line Seen in U.S. Spying on Companies*, NEW YORK TIMES, May 21, 2014, at A1.

[35] Of course, not all industries are equally susceptible to this sort of concern. In the production of large commercial airplanes, there are few American rivals to Boeing, for example. And yet officials frequently summon the example of Airbus and Boeing in illustrating the norm's reach.

A second explanation emphasizes more generally the principle that government agencies should not subordinate their official missions to the economic preferences of the market. But pitched at a high level of generality, the theory is hard to sustain. Throughout the government, including in the national security area, official missions include lobbying on behalf of American firms in competitive industries. The Department of Commerce counts this as one of its core functions.

Perhaps the most theoretically rich account of the norm is the one recently advanced by Jack Goldsmith. He argues that:

> On the whole the United States doesn't gain much from stealing trade secrets from foreign firms to give to U.S. firms. But the United States and its firms have a lot to lose when other nations engage in this discrete form of economic espionage against U.S. firms. Thus the best rule for the United States is one that tries to limit this form of economic espionage. However, economic espionage outside this narrow context – not in order to benefit discrete U.S. firms, but rather to advantage the United States economy and U.S. firms generally on the global scale (in trade negotiations, e.g.) – serves U.S. interests, especially since the USG has the most powerful capabilities in this context. And so the USG thinks this form of economic espionage is acceptable.
>
> It is not surprising that the United States would seek to craft a nuanced rule about economic espionage that serves its interests. This happens all the time in international affairs. Nor is it surprising that so many nations are unimpressed with the United States' attempt to limit the one form of economic espionage (theft of foreign corporate trade secrets to give to a local firm) that so obviously harms U.S. interests, especially since the United States engages in other forms of economic espionage.

Goldsmith's realism is bracing and provocative. But the analysis (to be fair, presented in a blog post, rather than a scholarly article) raises a number of questions. First, on its own terms, the analysis presupposes that the U.S. national interest is served by announcing a rule that few other nations adhere to. Implicit in Goldsmith's account must be a view that the United States can, by articulating the norm, ultimately persuade or pressure other countries to follow suit. But there is no evidence to suggest that that has happened or that the norm is amenable to export.[36] Second, insofar as Goldsmith's realist account aims to explain the divergent interests of the U.S. and China, it pays insufficient attention to the fact that China is not necessarily the leading example of a country that organizes its affairs differently from the United States. According to leaked diplomatic cables of U.S. officials, French economic espionage causes more economic damage to its allies than Chinese or Russian espionage.[37] Third, the realist view, by emphasizing the role of the norm in the context of an ongoing cyber-contest between the United States and China, cannot explain for the norm's emergence in a pre-internet world and its staying power over a period of over forty years. So at best Goldsmith's account offers a plausible reading of the norm's present, but not its past.

---

[36] Cf. Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014) (arguing that the best opportunities for bridging the international digital divide lie with an "interactive norm-building process" of international socialization, through learning and imitation.)

[37] See http://www.cbsnews.com/news/wikileaks-france-leads-russia-china-in-industrial-spying-in-europe.

IV.

We are back, then, with a puzzle: Why this particular norm, concerning which American officials can often come across as moralistic? I argue that institutional culture, especially in the CIA, has a large role to play in rounding out our understanding of why the norm came into being and why it has endured.

Two key cultural factors are relevant. On the one hand, the ethos of American spies – especially in the CIA – has traditionally elevated the work of intelligence above the pedestrian affairs of the market (or, for that matter, the balance of the government). No doubt in part because of the early influence of WASPs, or the subsequent prominence of orthodox Catholics (and more recently, Mormons), the role of American spy has been shaped by a culture of secret societies and rituals. In the context of that culture, the norm makes a lot of sense, ensuring that the sacred work that spies undertake is not somehow profaned by the workings of the market. To spy in order to benefit private firms would be to misunderstand the value hierarchy of the intelligence cult.

At the same time, the same individuals who elected to serve in this elite society had respect for – and frequently deep experience in – the market, especially on Wall Street. As former securities lawyers and investment bankers, they had faith in the integrity of the private market and regarded its smooth operation as natural and desirable. The norm thus also reflected a cultural ethic of confidence in capitalism and economic fair play. The CIA could – and did – have extensive dealings with business, but the lines would be drawn in such a way that the business firms were essentially supporting the intelligence professionals, and not vice versa.

These two cultural features of American intelligence – a belief in the superiority of national security to the market and a concomitant commitment to free-market values – help to explain American exceptionalism in this area. On the first dimension, although cultures of secrecy define all intelligence agencies, European spies are not as differentiated from the ordinary civil service as American spies are (or were). The CIA, which, in comparison to European counterparts, is a relatively new organization, self-consciously established itself as an elite organization, recruiting on Ivy League campuses and embodying a noblesse oblige approach to public service. (In its analytic function, the CIA aspired to another American institution with an ambivalent relationship to the market: the research university.) American spies – especially in the early years – regarded themselves as fundamentally different from ordinary American civil servants. And by and large, they were correct in their self-assessment. Second, the CIA came into being in the decades of extraordinary American economic productivity around the world. Whereas American spies took for granted American economic prowess, counterpart officials in Europe operated with decades of experience of economic highs and lows, not to mention greater political appetite for more regulated markets, in their societies.

It would be too much to claim that the entire historical record bears out the cultural theory of the norm. But certainly some key moments in the norm's career are illuminated by it. For example, it makes sense that the norm would have been initially threatened by Admiral Stansfield Turner, a career military officer who failed to earn the trust of career CIA officers as President Carter's CIA Director. Alarmed by the first serious (and politically salient) threat to American economic hegemony in the post-WWII period, Japanese car manufacturing, Turner's approach might well have made economic sense. But it was a cultural non-starter within the CIA, as Turner came to appreciate when his senior staff discouraged him from making this change. Furthermore, the cultural account helps to explain why the post-Cold War CIA declined the invitation extended by a number of congressmen to maintain the agency's ongoing relevance by pivoting into

economic espionage. Such a move would have offended the traditional CIA officer's sense of the right ordering of the intelligence domain. The cultural account also makes of the recent push to locate the norm in a more formal, outward facing legal document (PPD-28). Such formalization makes sense in that the norm was being explicitly exported to a culture (NSA) very unlike that of the CIA, where the norm originated.

The centrality of culture to understanding behavior in matters of national security has been emphasized by scholars before. For example, Jeffrey Legro identifies areas in which the cultural preferences of the British and German militaries powerfully shaped military and policy choices during WWII.[38] And Ryan Goodman and Derek Jinks have employed a cultural account to make sense of the norm against assassination.[39] But the intelligence community, with its deliberately complex stance toward the rule of law, might have been thought to impervious to this sort of norm generation. In an age in which the governance of intelligence agencies is in flux, and new institutional designs are being debuted, it bears consideration that cultural organizational factors will inevitably shape the degree to which these reforms take root and ultimately prove effective. The project of governing intelligence ought, at a minimum, to be attuned to the fact that the intelligence community (or specific agencies within it) comes to oversight not as a regulatory tabula rasa but as a corporate body with inclinations to self-regulate in certain areas (but not others).

V.

Will the norm endure in the age of cyber-security? The relationship between culture and the larger strategic environment is complex. Over the last 15 years during which counter-terrorism has dominated the agenda of the American national security state in general and the intelligence community in particular, American spy agencies have undergone profound change. For example, commentators have noted that in the post 9/11 period, the CIA's culture has become increasingly defined by its paramilitary function. Whether or not this represents a return to an authentic institutional identity that characterized CIA's predecessor agency OSS, it certainly represents a profound change in the sensibilities of the Cold War spy agency that privileged espionage and analysis, not targeting and killing.

More change is afoot. On the institutional level, CIA Director John Brennan recently undertook to fundamentally alter the way the CIA is organized, placing analysts and spies in much closer proximity than they have traditionally been. More strategically, cybersecurity has arguably displaced counter-terrorism as the defining national security threat of the present moment. Even as surveillance authorities in the counter-terrorism domain are being curtailed, the intelligence community is redoubling efforts in the cyber-arena. The new push into cyber-security raises challenging questions about cultural change within the intelligence community and the viability of the norm more specifically. That is because cyber-security entails ever greater commitments to blurring the boundaries between public and private actors in the provision of national security.

The surveillance state (in particular, the NSA) has already been deeply implicated in public-private collaboration. Take, for example, Section 702 of the FISA Amendments Act which essentially a framework for public-private collaboration at the heart of the surveillance apparatus. And the NSA maintains an office that focuses entirely on the liaison function with private actors. But if anything the level of public-private collaboration in surveillance matters was relatively limited to corporate actors in the telecommunications and high-technology domains, as well as the traditional constituents of the defense-industrial base. The

---

[38] See JEFFREY W. LEGRO, COOPERATION UNDER FIRE: ANGLO-GERMAN RESTRAINT DURING WWII

[39] See Derek Jinks & Ryan Goodman, *Toward an Institutional Theory of Sovereignty*, STAN. L. REV. 1769-1772 (2003).

emergence of cyber-security represents an altogether new scale in the delivery of security as a joint public-private venture.[40] The breakdown of the divide between public and private actors in cyberspace owes most fundamentally to the fact that cyberspace is shared by the government and private actors.[41]

Consider, for example, the recently issued Department of Defense cyber security strategy document which clarifies that the private sector has a significant role to play in providing for national security in the cyber arena.[42] Pending legislation would immunize private actors for greater information sharing with the government, just as the FAA immunized private firms for their role in the surveillance world. And programs across the government, from the FBI[43] to the Department of Homeland Security[44] to the Department of Defense (as well as collaborations between multiple agencies[45]) emphasize the need for effective means of public-private collaboration on cyber-security issues.

Even as the cyber-security imperative places ever-greater pressure on the separation of market and the national security state, the government's (short-term) reaction has been (at least rhetorically) to double down on the norm. Thus, the White House's recently issued Executive Order that employs a sanctions regime to address the risk of cyber-hacking targets takes specific aim at those who seek to hack for private gain. Here is a clear message to the Chinese that hacking for private gain – a key strut of the Chinese pursuit of "indigenous innovation"[46] – is a non-starter for the American national security state.[47]

---

[40] In the wake of the Sony Pictures hack, the White House issued an executive order explicitly targeting North Korea based on its role in the hack.

[41] HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 113 & 170-184 (Cambridge University Press, 2005); see also, on public-private information sharing in the battle against cybercrime in the US and the UK, Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

[42] See also Department of Homeland Security website, "Combatting cyber threats is a shared responsibility. The public, private, and non-profit sectors, and every level of government—including DHS—all have an important role to play."

[43] "InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S." "350 of our nation's Fortune 500 have a representative in InfraGard."

[44] National Infrastructure Advisory Council, Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations, 17 (2008), *available at* http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf ("The Sector Partnership Model is one of the most comprehensive public-private partnerships undertaken by the federal government, engaging nearly every major sector of the economy and every level of government. It seeks to address the security needs and expectations of a variety of highly diverse businesses, government organizations, and security partners under a common framework.").

[45] Ellen Nakashima http://www.washingtonpost.com/world/national-security/cyber-defense-effort-is-mixed-study-finds/2012/01/11/gIQAAu0YtP_story.html ("The Defense Industrial Base cyber pilot includes 17 defense companies, among them Bethesda-based Lockheed Martin, which several years ago had terabytes of data related to the Pentagon's Joint Strike Fighter project stolen from its networks."); http://www.defense.gov/releases/release.aspx?releaseid=15266 (quoting then-Deputy Secretary of Defense Ashton Carter to the effect that "I am pleased by the deep collaboration between DoD, DHS and DIB partners. The success of this program encourages us to explore additional ways to enhance the protection of defense industry networks and DoD information.").

[46] Scott J. Shackelford, Eric L. Richards, Anjanette H. Raymond & Amanda N. Craig, *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 11 (2015); earlier at Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 162 (2014)

[47] Jonathan E. Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI.-KENT J. INTELL. PROP. 189 (2009).

But the attempted reinvigoration of the norm may prove ineffective against the advent of the American "market-state."[48] The cultural distinctiveness of the intelligence community has been steadily eroded by fifteen years of budgetary growth, bureaucratic reordering and outsourcing. As I have argued elsewhere, with an unprecedented commitment by the intelligence community to transparency and with the emergence of interest group politics in intelligence, the intelligence domain increasingly resembles the balance of the regulatory state. Accordingly the norm – and with it, the separation of the market and the state in intelligence matters – has never been on shakier footing.

[48] See generally PHILIP BOBBITT, TERROR AND CONSENT