H-Net Reviews
in the Humanities & Social Sciences

Amy B. Zegart. *Spies, Lies, and Algorithms: The History and Future of American Intelligence.* Princeton: Princeton University Press, 2022. Illustrations, tables. 424 pp. $29.95, cloth, ISBN 978-0-691-14713-0.

Reviewed by Mark Stout (Johns Hopkins University)

Published on H-War (October, 2022)

Commissioned by Margaret Sankey (Air University)

Amy B. Zegart, a senior fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies at Stanford University, is one of the most prominent scholarly voices on intelligence in the United States, so a new work from her is always worthy of attention. Her latest book, *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, follows a number of other works on related topics. Perhaps most notably, Zegart is the author of *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (2007). In that book, which attracted a great deal of attention, she looks at how the 9/11 attacks might have been thwarted and attributed the failure to do so to the incentives that operate on government officials, foot-dragging inside US intelligence agencies, and the fragmented structure of the federal government. Zegart is also the author of *Eyes on Spies: Congress and the United States Intelligence Community* (2011), which gives a gloomy assessment of the prospects for robust congressional oversight of intelligence. In addition, she has written on such topics as cyber operations and drones. Zegart brings all these strands and more together in her new book.

Zegart laid out her goals for *Spies, Lies, and Algorithms* in a February 1, 2022, interview on C-SPAN. First, she wanted "to provide an Intelligence 101." She went on to say that "the book was aimed at my students at Stanford and so I wanted to lift the veil on how the intelligence community really works because my students mostly get their education from the entertainment industry." Second, she wanted to "look at how emerging technologies like AI [artificial intelligence] are transforming every part of the threat landscape and the intelligence business." In response to a question as to whether American intelligence agencies are organized and functioning in a way that is appropriate to the threat the country faces, her answer was "not yet."[1] In this book, she succeeds in meeting her goals and is convincing in arguing that the intelligence community faces serious challenges.

Zegart writes her book with a deft hand and in prose devoid of scholarly jargon. In fact, she criticizes the US intelligence community for its use of "intelligence speak" when trying to communicate with the American public (p. 11). She notes that this had dire consequences in the case of Russian election meddling when the community was un-

able to convey to the public the dire nature of the situation.

The book has two major themes. The first is the relationship of the public and its representatives in Congress to intelligence. Included here are such topics as popular portrayals and understandings of intelligence, the democratization of intelligence, and the grim state of congressional intelligence oversight.

In a chapter that draws heavily on work that she did more than a decade ago, Zegart laments the "crisis in intelligence education and its costs" (p. 13).[2] She argues that "spytainment" has exercised a strong and pernicious influence on public and elite understandings of intelligence. She notes that Americans who consume spy entertainment tend to be more supportive of US intelligence agencies but also more willing to support aggressive counterterrorism tactics. She concludes that "mounting evidence suggests that fiction too often substitutes for fact, creating fertile ground for conspiracy theories to grow and influencing the formulation of real intelligence policy" (p. 43).

Zegart also laments the intelligence community's extensive overclassification and the broken state of the Freedom of Information Act. These factors, she says, contribute to the lack of scholarship on intelligence, though it is worth mentioning that she is referring only to political science not history or other aspects of intelligence studies. She also writes that a paucity of publicly available information contributes to a lack of undergraduate courses on intelligence. All this ignorance, she maintains, is another factor leading to dangerous conspiracy theories. In this vein, she closes by noting with some alarm that policy elites sometimes invoke fictional characters, such as Jack Bauer and his perpetually ticking time bomb. She says that "these ticking time bomb situations have never occurred" (p. 41). (To be slightly pedantic, she is wrong on this. Alistair Horne writes about one such occasion in his book *A Savage War of Peace*, but it is the exception that proves the rule; the senior French officer involved refused to have the suspect tortured and no bomb went off.[3])

The chapter on congressional oversight is no more uplifting. It largely summarizes Zegart's book *Eyes on Spies* and it explains how Congress has seldom provided good oversight of the US Intelligence Community because of the low perceived payoff to the politicians in Congress for serving on the intelligence community, a lack of intelligence expertise in the Congress, and the fragmented budget authorities governing intelligence.

The second, dominant, and more compelling theme of the book is the influence of technology on intelligence. Zegart argues that technology "is challenging American intelligence agencies in three profound ways" (p. 3). First, it is "generating new uncertainties" and empowering both state and non-state adversaries (p. 4). Second, "data volume and accessibility are revolutionizing sensemaking" such that the "intelligence playing field is leveling" and "intelligence collectors are everywhere and government spy agencies are drowning in data" (p. 6). Third, technological changes (one might add social changes, too) are forcing "intelligence agencies to engage the outside world, not stand apart from it" (p. 8). These are not problems that the government can grapple with by itself. Private companies are the main engines of innovation, and they have capabilities and data that the intelligence community may need. Yet there are tensions in these relationships: private companies compete for talent with the community, they make decisions about encryption that may be contrary to the community's interests, and they can sometimes be reluctant to cooperate with the intelligence community.

Zegart also addresses the democratization of intelligence, a phenomenon that we have seen in dramatic terms in connection with the war in Ukraine, which started about three weeks after the book was published. Democratization of intel-

ligence, as she describes it, is composed of three trends: increasing commercial imagery satellites and capabilities, including rapid revisits that are getting close to an ability to stare; "the explosion of connectivity and other open-source information on the Internet; and advances in automated analytics like machine learning" (p. 231). In an insightful chapter, Zegart illustrates how nongovernmental personnel are applying these kinds of capabilities to "nuclear sleuthing" in ways that are "fundamentally challenging U.S. intelligence" (pp. 14, 227). Such sleuthing, she warns, can be dangerous for multiple reasons. Nongovernmental sleuths "can inject errors in the policymaking world," as in 2011 when a class at Georgetown University got major press and governmental attention for what turned out to be an egregiously incorrect high estimate of the Chinese nuclear arsenal (p. 241). In addition, correct public analysis can bollix up diplomatic efforts by forcing premature action and "narrowing the range of face-saving political outcomes for each side" (p. 246). Finally, "clever nuclear sleuthing in the public domain can alert adversaries about weaknesses in their own camouflage, concealment, and deception techniques that they did not know existed" (p. 247).

Zegart concludes the book with a discussion of cyber threats, noting that they include "hacking both machines and minds" (p. 15). She observes that tech firms are sometimes reluctant to help the government deal with this issue and also argues that the "idea of a cyber threshold of war" has become irrelevant. Instead, she argues persuasively that cyber warfare today is more like covert action, "operating in the gray zone between war and peace without official government acknowledgement" (p. 258). She also comments on the long-standing tension between intelligence personnel who tend to prefer surveilling and understanding targets and warfighters who tend to prefer using intelligence to attack targets. Of course, this is a long-standing issue that, in a different domain, goes back to at least World War II and tensions between intelligence personnel who wanted to observe or turn foreign spies into double agents and J. Edgar Hoover's Federal Bureau of Investigation which preferred to arrest them.

The book addresses other issues that are not explicitly about the relationship of the public and Congress to intelligence or about technology. Nevertheless, the public and technology keep creeping in. One chapter, for instance, discusses espionage, reasons why people spy, ways intelligence service recruits agents in the digital age, and the difficulties of counterespionage. Zegart discusses the well-known statistical problems inherent in applying polygraph testing to an entire agency. She also lays out "three key counterintelligence challenges": excessive trust in the loyalty of one's own personnel (it might be added that it is entirely possible to place too much trust in the security of technology, too); Angletonian paranoia; and the fact that technology enables "bigger, faster, [and] better" breaches (pp. 164, 156)

A chapter on covert action is somewhat less satisfying. Zegart's discussion of why covert action can be appealing to decision makers seems to miss out on some of the explanations that political scientists and historians have brought to light in the last few years: domestic politics, a perception that covert action is inexpensive, and a desire not to be publicly seen to be violating international law.[4] In addition, she observes that "the more CIA [Central Intelligence Agency] people are hunting, the less they are gathering. Paramilitary activities, however successful they may be at taking terrorists off the battlefield, take time and resources away from the CIA's core job: giving the president decision advantage" (pp. 193-94.) This is a persuasive argument, though it seems rather less salient now that the United States finds itself focusing on near-peer competitors than it probably did at the height of the global war on terrorism.

Although this book breaks little new conceptual ground, it should be of wide interest to the public and will also be of use in higher education, as

Zegart intended. It does not attempt to be a fundamental nuts-and-bolts textbook à la Mark Lowenthal's *Intelligence from Secrets to Policy* (2000, 9th edition published in 2022). However, it would be an excellent complement to a book such as that. (I have already used portions of it in that way.) It will be useful to undergraduates whether they are political science students wanting some familiarity with intelligence issues, aspiring intelligence practitioners, or simply young people who simply wish to understand what the intelligence community is doing in their name.

All this said, it is not clear what kind of shelf life this book will have. Already the section about the role of spytainment seems a bit dated now that spy television no longer has the very prominent role in American life that it did a decade or more ago. One also wonders whether there might be some changes, albeit not for the better, in congressional oversight. In our present hyper-partisan era, might members of Congress start to seek assignments on the intelligence committees believing that they provide good platforms for smiting political enemies? Most important, however, the lion's share of this book is devoted to technological issues that are unfolding at a dizzying pace. Zegart may wish to produce a second edition in just a few years.

Notes

[1]. Amy Zegart, interview by Susan Swain, "Q&A," C-SPAN, February 1, 2022, https://www.c-span.org/video/?517614-1/hoover-institutions-amy-zegart-discusses-espionage-threats-facing-us.

[2]. Amy Zegart, "'Spytainment': The Real Influence of Fake Spies," *International Journal of Intelligence and CounterIntelligence* 3, no. 24 (2010): 599-622.

[3]. Alistair Horne, *A Savage War of Peace: Algeria 1954-1962* (New York: Penguin Books, 1985), 203-4.

[4]. Michael Poznansky provides a useful catalog of explanations in Diane Labrosse, ed., "H-Diplo Roundtable XXI-43 on Cormac. Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy," H-Diplo, H-Net, May 25, 2020, https://networks.h-net.org/node/28443/discussions/6165505/h-diplo-roundtable-xxi-43-cormac-disrupt-and-deny-spies-special.

If there is additional discussion of this review, you may access it through the network, at https://networks.h-net.org/h-war

Citation: Mark Stout. Review of Zegart, Amy B. *Spies, Lies, and Algorithms: The History and Future of American Intelligence.* H-War, H-Net Reviews. October, 2022.

URL: https://www.h-net.org/reviews/showrev.php?id=57755