University of Nebraska Omaha

Space and Defense

Volume 14
Number 0 *Volume 14 Issue 1 Spring 2023*

Article 10

May 2023

Book Review: Spies, Lies, and Algorithms: The History and Future of American Intelligence

Claire Benedix
University of Nebraska at Omaha, cebenedix@unomaha.edu

Recommended Citation

Benedix, Claire (2023) "Book Review: Spies, Lies, and Algorithms: The History and Future of American Intelligence," *Space and Defense*: Vol. 14: No. 0, Article 10.
DOI: 10.32873/uno.dc.sd.14.01.1053
Available at: https://digitalcommons.unomaha.edu/spaceanddefense/vol14/iss0/10

Amy B. Zegart, Spies, Lies, and Algorithms: The History and Future of American Intelligence (Princeton University Press, 2022), 276 pp.

Claire Benedix*

The security environment is entering a new threat landscape; one that must be fought in both the physical and virtual world. The seemingly instantaneous progress of digitization and the cyberspace domain threatens to destabilize traditional warfare strategies and intelligence norms. Amy Zegart, an American academic and leading national security expert, outlines the history and future of American intelligence with a specific emphasis on emerging cyber threats in the digital age. In Spies, Lies, and Algorithms, Zegart explains the roles of technological breakthroughs in a world of big data by chronicling the history of intelligence education and organizational reform, the evolution of American intelligence, what intelligence is and is not, the challenges of intelligence and counterintelligence analysis and covert operations, legislative responsibilities, the upsurge of non-state actors, and the advancement of cyber threats.

Spies, Lies, and Algorithms serves as a comprehensive guide and essential resource for intelligence and security practices in the cyber age, while remaining accessible to a layperson audience. Although centered around often jarring topics, Zegart tackles complex concepts by broadening their scope to guide the reader through the fundamental components and core theoretical principles of intelligence tradecraft and the evolving nature of information operations, emerging technologies, and cyber threat intelligence. Zegart's account of the United States' past, present, and predicted future intelligence posture confronts critical concerns that are sure to arise from the new reality developing in the cybersphere.

Zegart seeks to learn from past intelligence failures; she proposes that by analyzing past and present intelligence trends and technologies, experts can forecast organizational challenges and cyber risks that require modern solutions. Her research looks ahead at the future of intelligence and how the United States can not only mitigate these subsequent cyber threats but accelerate our own intelligence posture. Yet, responding to these organizational challenges and filling knowledge gaps is no easy feat. She describes a plethora of variables that explain why American intelligence models and traditional spycraft are becoming obsolete. This emergence of unconventional techniques is giving rise to a game-change era of warfare: one without a rule book.

The cyber world is transforming modern power dynamics by negating outdated assumptions within power structures and relationships. The first few chapters explore how power is no longer defined solely by military dominance, rather it is now measured through multifaceted approaches in which education and training,

advanced technology, and innovative science and engineering enhances tactical dominance. Zegart emphasizes how this disruption to conventional warfare not only upsets the principles of military doctrine but also broadens an adversary's battleground. Cyberspace provides nation states and non-state actors with a relatively unregulated landscape of information that allows them to interact and exchange data with internet connected devices, software, or networks around the world, also known as the internet of things (IoT). This new dimension of virtual connections and electronic mediums has the power to influence society with a direct impact on individual and state security. These contemporary security components are necessary in order to remain competitive in cyber activities, yet they also trigger additional vulnerabilities and targets beyond the domains of traditional defense tactics.

The cybersphere hosts an ecosystem of diverse individuals, communities, infrastructure, and networks that carry out cyber attacks in the shadows. Throughout her research, Zegart highlights the five most common types of cyberattacks which are: stealing, spying, disrupting, destroying and deceiving. Although conducted virtually, all five attack types have the potential to target the physical world. These "unprecedented demands on intelligence" may include attacks on critical infrastructure, theft of sensitive customer or personal identifiable information (PII), or economic espionage that may spur doubt and distrust through secretive operations, which is why Zegart asserts that these cyber threats have everything to do with intelligence (pp. 269). The novel nature of these cyber attacks, paired with bureaucratic shackles and lagging modernization efforts, may neutralize the intelligence community and law enforcement's offensive and defensive cyber capabilities or approaches, which in turn, impacts how well decision and policymakers can operate. This cyclical failure to acclimate, incorporate, innovate, and progress only contributes to the previous patterns of U.S. reactive intelligence.

Zegart notes that cyber threats are not always direct attacks, nor are they always orchestrated by state-sponsored actors, cybercriminals, or notorious hackers. Instead, the cybersphere allows for any individual to operate under the guise of anonymity with the right resources. Zegart argues this new era of unconventional warfare methodology and incognito, malicious behaviors should be an intelligence priority. Users may manipulate groups or individuals through cyber espionage to undermine a state's stability, security, and performance through fake profiles and throwaway accounts, secure VPN encryption, bots, and a growing list of emerging technologies. Zegart stresses the severity of interference and spying efforts which can range from Russian operatives impersonating Americans and spreading propaganda through social media platforms to direct interference in presidential elections.

Information-based geopolitics create intangible data-sourced advantages that may be exercised remotely. These new age assaults challenge the status quo of state

sovereignty and territorial integrity, while generating more questions and uncertainty surrounding the aggressor's intentions and capabilities and the victim's vulnerabilities. Zegart utilizes the example of Russian trolls fueling political discontent through their interference in American-targeted social media groups on platforms such as Facebook and Twitter in order to incite domestic instability or violence, spread disinformation, and gather unauthorized data such as user names and passwords. This influence can be weaponized to target specific states, businesses, and individuals through information warfare campaigns. Zegart argues that a paradigm shift is necessary as a state's ability to incorporate, mobilize, and respond to these elements will be a determining factor in the success of modern intelligence and warfare.

From drones and Google maps to deep fakes and weaponized social media, Zegart warns how accessible computing power, connectivity, and open source information overloads are blurring the lines of conventional warfare and deterrence. These gray zones and expanding attack vectors can both benefit and jeopardize strategic positioning through increased ambiguity surrounding cyber, military, and hybrid doctrine, while muddling the differences between spying and attacking. These increasingly unclear norms make it difficult to navigate an actor's intentions and resources, especially when operating under stagnant intelligence culture or inflexible priorities.

Zegart's digestible overview of intelligence policy and spycraft addresses the structural and technological shortcomings the intelligence community has and continues to face by weaving together historical examples and previous research with the latest commentary on cyberspace security issues, American policymaker interests, and the ever changing threat landscape. Although Spies, Lies, and Algorithms does not delve into the technical and operative intricacies of how many of these cyber threats such as machine learning (ML) and artificial intelligence (AI) function, the investment strategies required to leverage and integrate these emerging technologies through private-public collaboration, or how the intelligence community can create sustainable, yet competitive, technological research and development incentives, Zegart still provides the reader with a great introduction to the unprecedented technological advancements sweeping the world and the necessary tools to adequately understand past, present, and future American intelligence challenges as well as possible opportunities to overcome them.

***Claire Benedix** attended the University of Nebraska at Omaha and graduated with a BA in International Studies with a concentration in global strategic studies and Political Science with a concentration in foreign and national security affairs. She graduated with her MS in Political Science with an international affairs concentration and a certificate in intelligence and national security from the University of Nebraska in May 2022. As a graduate assistant with the National Counterterrorism, Innovation, Technology, and Education Center (NCITE), she spent two years researching training and education research and implementation strategies in the U.S. intelligence

community with a specific emphasis on technological and cyber training standards and practices. Her research interests include the implications of politicized intelligence and American intelligence culture reform.