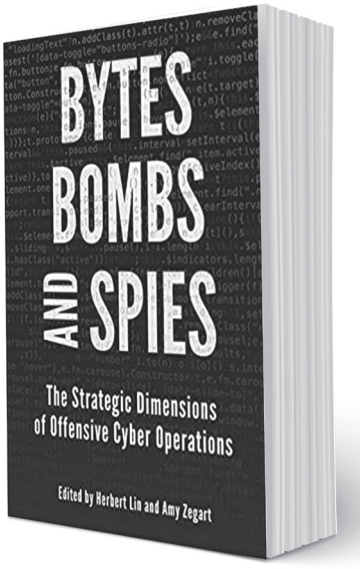
Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations

Edited by Herbert Lin and Amy Zegart



Reviewed by
Cadet Annalise Callaghan
Dr. Jan Kallberg

EXECUTIVE SUMMARY

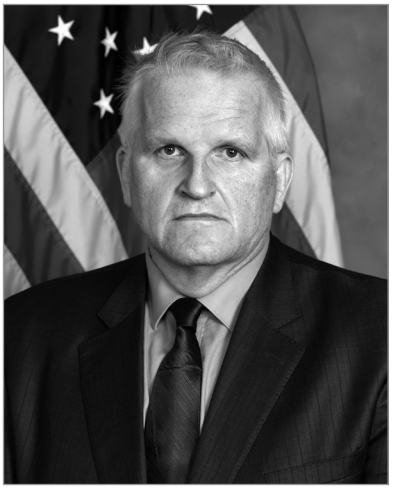
The following book review explores the content and insights of Dr. Herbert Lin and Dr. Amy Zegart's *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Initially published in 2018, the book is composed of a collection of works by prominent cyber scholars, practitioners, and professionals on the strategic uses of offensive cyber operations. This review begins with a contextualization of the circumstances that inspired the editors to convene the featured experts to collaborate on the book with the ultimate goal of filling the critical gap in conceptual thinking that has, to date, lagged behind the development and engineering of cyber technologies. The review proceeds by sorting the book's works into four interrelated themes pertaining to offensive cyber operations: (1) strategy and doctrine, (2) operational considerations, (3) escalation dynamics and deterrence, and (4) the role and relationship of the private sector. These subsections attempt to identify the book's variety of authors' academic and professional backgrounds – the diversity in these backgrounds and the prevalence of not only academic tenure but also practical experience serve as one of the book's unique strengthening characteristics. Within each theme, the review then provides a synopsis of the authors' various analyses in their respective works. The book that emerges as a product of these analyses and contributions traverses new territory in cyberspace thinking, addressing the strategic cyber landscape's fundamental technical, political, historical, psychological, and legal dimensions. Accordingly, *Bytes, Bombs, and Spies* is a text worthy of a hall of fame certification.

Cadet Annalise Callaghan is a yearling at the United States Military Academy. She is a double major in International Affairs and Law and Legal Studies: her research focuses include politics and power in cyberspace, information warfare, political participation, international cyber law, and privacy law. She is a Dean's Writing Fellow; serves on the officer teams of the West Point Ethics Debate Team and Ski Patrol; and is a participating member of the Parliamentary Speech and Debate Team, Model United Nations, the Domestic Affairs Forum, the International Affairs Forum, the Civic Engagement Initiative, and the Student Council on United States Affairs, along with several cultural and diversity forums. CDT Callaghan is originally from Eagle River, WI, and Houghton, MI. Upon graduation, she hopes to branch Cyber or Military Intelligence.

REVIEW

It was 2008 when centrifuges first began to malfunction at the nuclear facility in Natanz, Iran. The plant employees were perplexed when control room records indicated business as usual – none of the signals pointed to equipment failure. Some were fired; others were physically staged to oversee centrifuge performance and report their observations. Stands of linked centrifuges were carted away under suspicions of poor engineering, incompetence, and sabotage. It was not until two years later that the culprit – a computer worm that quickly became known as Stuxnet – accidentally emerged on the global stage. In the weeks that followed the computer worm's initial discovery, several new variants were directed at the Iranian nuclear plant in Natanz at close intervals, culminating with the temporary impairment of nearly one-fifth of the facility's nuclear centrifuges. The exposure and emergence of what can be considered the world's first significant cyber weapon and the engineering of its deployment (at least in part) by US forces would have profound implications for the decade that was to follow. Today, the utilization of Stuxnet by US and Israeli forces in Operation Olympic Games is widely credited with the slowing of Iran's progress toward the generation of a nuclear weapon: the extent to which it truly did so – and the questions regarding the operation's broader impact on US political and strategic power – remain.

One of the most notable aspects of Stuxnet's emergence was its reflection of the increasingly prominent roles that offensive cyber operations were coming to play in both US policy and international security. In the years following its discovery, however, the necessity of conceptual thinking to realize and articulate the effects of offensive cyber operations on the world was all but ignored. This fundamental gap in the literature on cyberspace served as the impetus for Dr. Lin and Dr. Zegart – Senior Fellows at Stanford University's Center for International Security and Cooperation – to host a



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's Degree in Political Science from the University of Texas at Dallas, and a J.D./LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities, especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

research workshop at Stanford in 2016, uniting distinguished researchers and professionals from the US military, intelligence, and policymaking communities to illuminate the critical dimensions of offensive cyber operations. They deliver the culmination of that collective effort in the book *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* The chapters in the volume underscore the emergence of four interrelated themes regarding offensive cyber operations: (1) strategy and doctrine, (2) operational considerations, (3) escalation dynamics and deterrence, and (4) the role and relationship of the private sector. In doing so, the book significantly advances the literature on the technical, political, historical, and legal dimensions of offensive cyber operations.

The first thematic category of the book is introduced by Chris Inglis, the former Deputy Director of the National Security Agency. In his segment, he identifies the roles of intelligence, surveillance, and reconnaissance in cyberspace, arguing that the need for persistence in all three categories is both operationally justified and constrained by legal and structural factors of society. He underscores the challenge of ambiguity in cyberspace, particularly concerning intent, and elaborates on how domestic and international law can necessitate restraint in military operations. Inglis concludes by providing recommendations for measures that can be taken by government departments and agencies to reconcile conflicting goals in the cyber domain while improving the overall intrinsic power of intelligence, surveillance, and reconnaissance efforts. Inglis is followed by George Washington University professors Henry Farrell and Charles L. Glaser (a former member of the Pentagon's Joint Staff), who explain how effects, saliencies, and norms should influence US cyberwar doctrine. They argue that understanding the focal points of adversaries is critical to anticipating their interpretations of offensive cyber operations by the US. They go further by demonstrating the implications this

premise has for diplomatic potential and cyber policy development. Dr. Max Smeets and Dr. Lin follow this analysis with an overview of U.S. Cyber Command (USCYBERCOM) strategy and recommendations for enhancing command capabilities, emphasizing the importance of prioritization and operational speed. Their scenario-based analysis of the command's strategy provides a compelling framework for the analysis of the potential outcomes it may yield. These three subsections provide comprehensive insight into the roles and impacts of strategy and doctrine in offensive cyber operations.

Dr. Austin Long, a Senior Political Scientist at the RAND Corporation, initiates the book's discussion on the operational considerations of offense in cyberspace. He contemplates the circumstances in which strategic influence can constitute a strategic attack in cyberspace and employs analysis of nuclear planning processes to frame his approaches to organizational planning, execution, and deterrence. The U.S. Naval Academy Keyser Chair of Cybersecurity Studies, Dr. Martin Libicki, builds upon the conversation by pointing out that adversaries are likely to learn from and adapt to US-based cyber operations: the effectiveness of secondary operations, he argues, is a function of how well initial operations can be designed to mitigate opportunities for enemy adaptation. Dr. Lin provides a survey of possible approaches to hacking a foreign adversary's missile development program. Long, Libicki, and Lin's respective works yield important deductions regarding the design, organization, and execution of major operations in cyberspace, especially when those operations pursue specific strategic goals.

Six chapters of Lin and Zegart's book are dedicated to the theory and analysis of escalation dynamics and deterrence in cyberspace. Discussion of these themes is grounded by five types of escalatory pressures: intelligence collection, commingling of assets for command and control, inappropriate rules of engagement and scope, public opinion, and unintended damage. Jason Healey – the Founding Director for Cyber Issues at the Atlantic Council – begins this discussion by pointing out that cyber conflict is often more escalatory than deterrent. With special emphasis on the Iranian response to Stuxnet, several case studies identify the security dilemma inherent to states' behavior as they perpetually work to increase their respective cyber capabilities. Erik Gartzke and Jon Lindsay also subscribe to this view, adding distinctions between cyber operations directed towards counterproliferation and preemptive counterforce, along with the insight that offensive cyber operations against nuclear weapons systems raise the risk of nuclear war. The following chapter reports on research – conducted by Michael Gross, Daphna Canetti, and Dana Vashdi – regarding the psychological harms and negative impacts of offensive cyber on attitudes and opinions – specifically on public confidence in national institutions. Steven Bellovin, Susan Landau, and Herbert Lin follow this by articulating the fact that appropriate intelligence can yield possibilities for discriminatory cyber-attacks: in other words, operations that limit damage to their targets. The twelfth chapter of the book, written by Michael Sulmeyer, C. Robert Kehler, and Herbert Lin, expounds upon the legal constraints identified by Chris Inglis at the beginning of the book, identifying the characteristics of operations in cyberspace that complicate the formulation of policy and rules of engagement.

Adam Segal draws upon these five chapters to compose a prospective case study addressing the potential for cyber escalation in a military confrontation between the US and China.

The fifteenth and sixteenth chapters of this book come to opposite conclusions regarding the private sector's role in offensive cyber operations. While David Aucsmith argues for the necessity of legal reform that would enable private companies to take offensive action consistent with the law of armed conflict, Lucas Kello contends that the capacity of such private action to upset international conflict stability and to put innocent third parties at risk constitutes too great a danger to be ignored. Irv Lachow and Taylor Grossman conclude the book with an objective overview of the private sector's role in supporting offensive cyber operations in government.

CONCLUSION

Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations fills critical gaps in the literature on offensive cyber operations to date, addressing fundamental technical, political, psychological, and legal dimensions of the strategic cyber landscape. The book's strength is underscored by its diversity of perspective and analysis by esteemed researchers and academics in the field, among whom professional experience working in government and security-related positions is notably prevalent. The book's internal validity is enhanced by the interconnectedness of arguments that fall under different themes, though it occasionally misses opportunities to substantively discuss contradictions between the array of theoretical frameworks it espouses. Frameworks for determining and measuring the effectiveness of offensive cyber operations constitute a critical gap in the literature, and should be pursued in future research. Despite the applicability of the literature in this book to the Stuxnet case study, for instance, the weapon's ultimate effectiveness is its most hotly debated and contested variable. It is also the one that poses the most significant strategic, ethical, political, and legal questions concerning the future offensive cyber operations. Defining a framework for the measurement of operational effectiveness has the potential to inform offensive cyber strategy – and subsequently, to influence cyber effects – for generations to come. The knowledge and analysis provided in *Bytes, Bombs, and Spies* contributes to the necessary foundation for such an endeavor to be pursued.

Title: ***Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations***
Publisher: Brookings Institution Press (January 15, 2019)
Paperback: 426 pages
Language: English
Paperback ISBN 978-0-8157-3547-2
Ebook ISBN 978-0-8157-3548-9
Price: $45.99 Paperback
$19.79 Kindle Edition