BOOK REVIEW ROUNDTABLE:

Information Technology and Military Power

Feb. 1, 2022

Table of Contents

1. Introduction: Innovators, Users, and Bureaucrats: Technology in War

Taylor Grossman

A cynical attitude toward technology is certainly nothing new in military analysis. Naysaying is a perennial accompaniment to technical change in warfighting, from early reactions to the machine gun to some of the current rhetoric around unmanned aerial vehicles.[1] You can find echoes of this strain of thought in almost any contemporary analysis of conflict: examinations of the American withdrawal from Afghanistan, overviews of the Russian military threat, explorations of U.S.-Chinese competition, and so on.

In the first chapter of *Information Technology and Military Power*, Jon Lindsay offers a concise but rich outline of the underlying scholarship on military innovation and effectiveness, including the classical Clausewitzian "fog of war" school of thought, and the related view of the impermeable chaos of the battlefield.[2] Lindsay's new book describes the persistent and cyclical challenges that seem to plague the American warfighting community, despite — or perhaps even because of — supposedly revolutionary achievements in technology.[3] Lindsay asserts that "information technology becomes more complex and increasingly essential for military performance without, however, providing any lasting decisive advantage on the battlefield."[4] The advent of modern computing has proved no different. "[W]ar," he writes, "has neither changed its nature nor become any more decisive in the information age."[5]

Yet, Lindsay's work is much more than a simple rebuke of the technology theory of victory. Lindsay's deeper contribution, something the reviewers in this roundtable agree about, lies

[1] See, for example, John Ellis, *The Social History of the Machine Gun* (London: Croom Helm, 1975); and John Kaag and Sarah Kreps, *Drone Warfare* (Cambridge: Polity, 2014).

[2] Lindsay, *Information Technology and Military Power*, 21–22. On the Clausewitzian approach to war, see Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976).

[3] Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020).

[4] Lindsay, *Information Technology and Military Power*, 11.

[5] Lindsay, *Information Technology and Military Power*, 67.

in offering an expansive framework for charting how organizations adapt and reform their information systems as new technologies emerge. He does this by focusing on the iterative, relational nature of information collection and analysis — the points of interaction between humans and technology. In Lindsay's analysis, information itself is best understood "not simply in terms of bits and bytes but rather a system of pragmatic relationships (between representations and referents, format and meaning, text and context, humans and computers, users and designers, allies and enemies, etc.)."[6]

The Argument

Lindsay's main argument lays out four types of information practice based on the interaction between two key independent variables: (1) the nature of the external operating environment, which he denotes as "constrained" or "unconstrained"; and (2) the internal solution set advanced in response, which he classifies as "organic" or "institutionalized." Lindsay's dependent variable is the resulting "information practice," what he defines as "the sociotechnical pattern of organizational behavior that coordinates the relationships between internal representations and the external world."[7] From his typology, Lindsay argues that the best situations arise from a well-defined problem and a well-structured solution, which he terms "managed practice."[8] Lindsay uses the example of the British Royal Air Force in early World War II to explore this type of practice, explaining that military leaders faced a fairly straightforward external problem set: defending the island from invasion. The air force developed a centralized internal structure to process "systematically constrained" intelligence about German *Luftwaffe* bombers, leading to a relatively effective Fighter Command that was able to triumph in the Battle of Britain by not losing.[9]

The second-best information practices result from unconstrained problems that are addressed with organic solutions, resulting in "adaptive practice."[10] Such scenarios are

[6] Lindsay, *Information Technology and Military Power*, 7.

[7] Lindsay, *Information Technology and Military Power*, 34.

[8] Lindsay, *Information Technology and Military Power*, 57.

[9] Lindsay, *Information Technology and Military Power,* 84, 101–08.

[10] Lindsay, *Information Technology and Military Power*, 62–63.

often tricky to balance, as they rely on a degree of decentralization that makes replication difficult. However, his case studies are replete with examples of organic user innovations that prove useful, at least on a small scale. Lindsay's chapter on drone campaigns demonstrates how practitioner-instigated changes led to tactical improvements, such as increased targeting accuracy and reduced casualty numbers.[11]

Suboptimal information practice results from poor calibration between the task at hand and the organizational infrastructure built to surround it. "Mismatches," Lindsay writes, "become more likely when the environment is dynamic or ambiguous yet the organizational culture is rigid."[12] Similarly, information practice devolves when organizations adopt independently designed solutions that become mired in specific quirks of personality or bureaucracy, rather than efficient, shared solution sets.

This seemingly simple framework, however, belies a much more nuanced picture of organizational evolution and adaptation. As Lindsay himself concedes, there is a degree of endogeneity inherent in his framework, as iterative feedback between the operating environment, the internal solution set, and the maneuverings of the adversary mean that the causal arrow can run the opposite direction — in other words, one adversary may cause the external environment to shift based on the solutions adopted by his or her opponent. As such, his key insights stand out more clearly in the four case studies that comprise the bulk of the book. While all three reviewers in this roundtable find Lindsay's analytic structure compelling, they draw different conclusions about the utility and generalizability of his theory, based on his case selection.

The Reviews: Case Studies and Policy Lessons

After giving a brief overview of Lindsay's theoretical framing, Susan Landau focuses on Lindsay's four case studies. The cases differ quite broadly in structure. While the first case on the Battle of Britain focuses on a discrete time period and conflict, each of the other three cases span years, and even decades, of technical and organizational evolution, often

[11] Lindsay, *Information Technology and Military Power*, 180–211.

[12] Lindsay, *Information Technology and Military Power*, 59.

across multiple conflicts. The first case also offers a fairly straightforward comparison of two organizations, the Royal Air Force and the German *Luftwaffe*, whereas the latter three cases focus almost entirely on the American military establishment.[13]

For Landau, Lindsay's level of detail is both a strength and a weakness, as it refines the overarching analytic model while also muddying some of the book's conceptual clarity (and perhaps its appeal to a non-expert audience). All four cases offer valuable insights and perspectives, often informed by Lindsay's own tenure in the military. However, to Landau, Lindsay's second case study on FalconView, a mapping and planning program that grew to prominence in the 1980s and 1990s, is his strongest. She notes that this chapter "stands out because of the clarity with which Lindsay describes two critical issues: how user needs drove the design of FalconView … and the conflicts between user-designed systems and military bureaucracy." The last two cases, in her view, are mixed successes. Lindsay's study of special operations in Iraq, Landau writes, is overly detailed, and thus ultimately "less compelling," while the final case on drone operations has some "distracting" tangents on legality and executive oversight that cause it to "wander."

Yet, although she has some quibbles, Landau ultimately finds the book impressive. She is especially supportive of its reminders that "no matter how powerful IT may be, understanding how it is used requires a human-centric approach." This central thesis, Landau notes, is usefully drawn out through Lindsay's collection of historical cases.

Derek Reveron takes a broader view of Lindsay's work. Like the other two reviewers, he finds the book's focus on the human elements of information practice a refreshing and important contribution to the literature. Reveron praises the work's scope, noting that the book is "truly an interdisciplinary work, covering topics in security studies, political economy, cognition, science and technology studies, and organizational theory." The cases, he adds, are particularly strong, as is Lindsay's dual-hatted lens as both a practitioner and as a scholar.

[13] Interestingly, both Landau and Derek Reveron note in their reviews that Lindsay's appendix on methodology offers useful insights on case selection that would have been more helpfully placed in an introductory chapter.

Reveron does offer several critiques of the structure and case selection. He notes that several of the recent cases could have been strengthened through more comparative work. The case on special operations in Iraq, for example, could have been paired with a chapter focused on conventional forces during the same time and in the same place. Such a case, Reveron believes, would have been useful in demonstrating "how the information practices of other militaries perform when operating within the same environment." Similarly, Reveron notes that comparative work across militaries operating in the same external environment — coalition partners, for example — could also help to draw out distinctions in the internal solution sets that lead to effective information practices. Finally, and perhaps most significantly, Reveron challenges Lindsay to look beyond the tactical and operational levels of warfare and to integrate his examination of information practice into a strategic understanding of organizations. While such questions were beyond the scope of the text, Reveron concludes that Lindsay is up to the task.

Jacquelyn Schneider focuses her review on the broader policy implications of Lindsay's work. Like Reveron and Landau, Schneider also values the analytic framework Lindsay constructs, which she notes is a "deceptively simple two-by-two theory." For Schneider, the level of nuance in the text is a positive: "While the theory is certainly elegant, it is Lindsay's ability to trace the complex interdependence of these variables that is the real contribution of the book."

Schneider finds Lindsay's takeaways "particularly timely for debates about information practice in contemporary U.S. defense policy." Where Landau hedges on the question of practical relevance, Schneider identifies direct applications from Lindsay's work to contemporary questions plaguing the American military. Although the United States has had a string of "tech-friendly secretaries of defense," promising research and development investments have rarely translated into battlefield successes. Lindsay's work demonstrates the shortcomings of both top-down and bottom-up drives for innovation in information practice. The FalconView case study is particularly salient in demonstrating the limits of user-based experimentation and the need to "link innovation and institutionalization." While this lesson may not be new, Lindsay provides a useful framework for demonstrating the persistence of such challenges across the Department of Defense.

Schneider is especially interested in the role of organizational identities in Lindsay's work. Despite flashy new acquisition programs targeting the start-up landscape, ingrained bureaucratic prerogatives often stymie effective information practice. Schneider points out that the case study on special operations in Iraq notably highlights the "important role that the masks of identity play by filtering information practice." Landau found this case less satisfying than the others. Schneider, however, singled it out as particularly useful in emphasizing the key pitfalls of the technology theory of war, especially when divorced from a deeper understanding of the role of culture and identity within military institutions.

Conclusion

Together, these three reviews highlight the many strengths of Lindsay's work: his rich analytic framework, detailed case studies, and robust insights into the shortcomings of innovation as an end unto itself. Like Schneider, I found myself most drawn to Lindsay's examination of organizational cultures. Lindsay is at his best when he is complicating traditional narratives of innovation and effectiveness. His cases serve as strong examples of the way cultural identities can distort and shape new technologies. Organizational structures often limit innovation potential, fitting new inventions into old processes. Lindsay's chapter on Iraq, for example, details the Navy SEAL culture of hyper-aggression and its effects on degrading the type and quality of information the organization mobilizes.

His four case studies are too distinct in both structure and subject to fully cohere as comparative applications of the analytic framework. Like Reveron, I found myself wishing for more directly comparative work. The first case on the Battle of Britain does an excellent job of examining how the British military tailored an institutionalized solution to address a constrained problem in a relatively finite period of time. Lindsay's subsequent cases address years and even decades of information practice evolution and often involve periods of both success and failure. The policy implications are simultaneously richer and opaquer: Lindsay's emphasis on cyclical evolution highlights how a well-honed solution can devolve as internal and external environments shift, but the factors that lead to improvement and deterioration are complex and often hard to pin down.

However, the breadth of the case studies helps illuminate a broad spectrum of information practice and organizational evolution. Throughout, Lindsay pays particular attention to the nature and structure of symbolic representation across information technologies, from the role of human operators in early radar systems to the nature of signature strikes in contemporary drone operations. Both measurement systems require simplification and shorthand, and both are shaped by tacit assumptions that people, not machines, made first. Organizational identities structure not only the way information is processed, but also the nature of information gathered in the first place. Technology is not neutral. Rather, it reflects the prerogatives of the people who make it.

Lindsay's final chapter delves into several of the big questions that foreign policymakers face today — competition and conflict with China, the future of nuclear warfare, and the role of cyber security and cyber operations. While this section encourages debate, it also serves to reinforce an important set of challenges to the evergreen technology theory of victory. As Lindsay puts it, "reliance on information systems is a Faustian bargain: the technologies designed to reduce uncertainty become new sources of it."[14] We would do well to remember this.

Taylor Grossman *is a senior research analyst and project manager in the Cyber Policy Initiative at the Carnegie Endowment for International Peace, where she works on cyber security and financial inclusion, cyber norm development, and other issues in technology policy.*

[14] Lindsay, *Information Technology and Military Power*, 217.

2. Decoding When IT Is Useful During Wartime — and What Causes IT to Fail

Susan Landau

Shortly before I read Jon Lindsay's excellent book, *Information Technology and Military Power,* I participated in a BBC broadcast on the Colonial Pipeline ransomware attack.[15] Although the book concerns the use of information technology (IT) in military actions — while the issue I addressed on the radio was possible Russian government involvement in the affair — the two topics share more than a superficial similarity. Both are about the fog of war created by the use of powerful IT in conflict creates — and our efforts to deal with it. Much has been written about how IT is changing the conduct of war. Lindsay attempts to bring structure to the discussion, and he is well equipped to do so: He comes at the work with an M.S. in computer science from Stanford; service in the U.S. Navy, including a deployment in Iraq; and a Ph.D. in political science. And, from the book's notes, Lindsay appears to have read most of the literature in the area. That breadth shows.

Lindsay's main contribution in *Information Technology and Military Power* is to argue that no matter how powerful IT may be, understanding how it is used requires a human-centric approach. IT is based on a sociotechnical system, and how effective it is depends upon how well organizations and people operate with the technology. That is something that those of us who do computer security know well, but it is a lesson that bears repeating. And it appears to be especially true in this domain. From Lindsay's description, it would seem that proponents of the "Revolution in Military Affairs" have not yet absorbed this crucial insight. At some level, that is no surprise, but what Lindsay does in *Information Technology and Military Power* is put meat on those bones. Through a number of in-depth case studies, Lindsay shows how this sociotechnical system actually works during war, delineating the evolution of the military's deployment of the technology and how adversaries adapt to each other based on how it is used. This provides a valuable set of lessons.

[15] Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020).

The Theoretical Framing

Naturally for a political science text, the book begins with theoretical scaffolding that examines how organizations in rapidly changing and dynamic situations manage their information practices. Lindsay first discusses the military's "external" problem, which can be constrained or unconstrained.[16] Constrained problems are those that operate within inherent limitations. These could be physical, social, technological — or some combination thereof. Unconstrained problems are more ambiguous with less clear limits and thus often present confusingly. Lindsay provides a number of examples of both: The Royal Air Force Fighter Command during World War II is a quintessential case of a constrained problem, while the German *Luftwaffe*'s strategic bombing campaign during that same conflict was unconstrained.[17] Next, Lindsay considers "internal" information solutions, which can be institutionalized or organic.[18] Institutionalized information solutions operate according to a set of clearly defined rules and controls. Organic solutions are much less hidebound — and thus also less predictable. Royal Air Force Fighter Command is an example of an institutionalized information solution (Lindsay explores this issue in depth), while improvised explosive devices represent an organic information solution.[19]

Having set up a standard social science set of variables, Lindsay asks what happens when constrained and unconstrained problems face institutionalized and organic information solutions. When a constrained enemy meets institutionalized information solutions, that is, Lindsay writes, a "managed practice" situation. Of course, the constrained enemy then changes its responses to less clear ones that use uncertainty as a strategy. This adaptation disrupts the institutionalized information response. Thus, the enemy has become unconstrained. The result is now that the military's responses are disjointed from the actions of its adversary. The military has, in Lindsay's words, been put in an "insulated practice" state. To be successful, the military must counter its adversary's changes by itself switching to organic information solutions, putting the situation in an "adaptive practice" mode. When this happens, the enemy adapts, using the best practices of its unconstrained

[16] Lindsay, *Information Technology and Military Power*, 7–11, 49–53.

[17] Lindsay, *Information Technology and Military Power*, 8.

[18] Lindsay, *Information Technology and Military Power*, 8–11, 53–56.

[19] Lindsay, *Information Technology and Military Power*, 8.

behavior. This response places the enemy in a constrained state, leaving the military's organic solutions less well suited to the situation. From the military's point of view, the situation is now in a state of "problematic practice."[20] Thus, the military will respond by moving back to institutionalized information solutions. The cycle then begins anew.

The Case Studies

After presenting the theory, Lindsay then moves to the heart of the book: its four case studies. These focus, respectively, on the Battle of Britain, user innovation in aviation planning software, the Revolution in Military Affairs, and drone warfare, the last three of which draw on Lindsay's own military experience. The other members of this roundtable are political scientists, so I will leave for them the task of evaluating Lindsay's theory and will utilize my expertise as a computer scientist to focus my review on the case studies.

Lindsay's choice of the Battle of Britain is, at first glance, a little surprising. After all, IT was in its infancy during World War II, and the issues that existed then were quite different from the ones we encounter today. But in his view, the case "was an obvious choice" because it involved "simpler technology," "a different war fighting domain," and had a "successful outcome." Moreover, the case is of "intrinsic historical importance" and there is "abundant archival data" to consult.[21] Such information would have been useful to have before the chapter began, as I found myself wondering why I was reading about IT's role in warfare at a time when it was only just developing. I did not wonder long, however, for Lindsay's writing in that chapter was captivating, and I was drawn in.

Lindsay details how the United Kingdom carefully measured everything it could. The most important technological development in this respect was radar, an area in which the country was operationally ahead of Germany.[22] London also relied heavily on visual observation. Indeed, Lindsay details how there were 1,000 observation points from which

[20] Lindsay, *Information Technology and Military Power*, 57–67.

[21] Lindsay, *Information Technology and Military Power*, 246.

[22] Lindsay, *Information Technology and Military Power*, 84–88.

observers were employed to spot incoming aircraft.[23] The British also relied on signals intelligence, which they used in both the air and at sea.

As Lindsay makes clear, the information the United Kingdom was able to collect and analyze gave it important strategic advantages over Germany.[24] The pilots may have won the battle, but thousands of personnel on the ground backed them up.[25] Lindsay's description of this case is not so much an illustration of the dynamics of cycling through different practices as it is an illustration of the power of information and data analysis, even when it is humans who are largely doing the analysis.

It is worth noting that the United Kingdom was — and evidently still is — assiduous about collecting data even before it was fully clear how it might use the information. During the recent pandemic, the country has been careful to collect genomic samples, which has made it easier to understand how the COVID-19 variants are spreading.[26] Likewise, the physicist Freeman Dyson has recounted how, during World War II, he helped calculate whether gun turrets on bombers saved flight crews' lives (they did not).[27] This work was based on data that compared survival with crew longevity. An additional paragraph in this chapter that described other similar uses of data would have been interesting and would have helped to provide historical context.

Lindsay's discussion of user innovation in aviation mission-planning software greatly benefits from the combination of his scholarly perspective with hands-on experience in day-to-day military operations. The chapter on this topic stands out because of the clarity with which Lindsay describes two critical issues: how user needs drove the design of FalconView —including, most critically, an easy-to-use interface that enabled novices to be productive quickly — and the conflicts between user-designed systems and military

[23] Lindsay, *Information Technology and Military Power*, 88–89.

[24] Lindsay, *Information Technology and Military Power*, 106–08.

[25] Lindsay, *Information Technology and Military Power*, 108.

[26] Harald s. Vöhringer et al., Genomic Reconstruction of the SARS-CoV-2 Epidemic in England, *Nature*, no. 600 (2021): 506, https://doi.org/10.1038/s41586-021-04069-y.

[27] Freeman Dyson, "A Failure of Intelligence: Part I," *MIT Technology Review*, Nov. 1, 2006, https://www.technologyreview.com/2006/11/01/227625/a-failure-of-intelligence/.

bureaucracy. Lindsay brings in valuable details about why FalconView was so popular. These include the importance of fitting the technology to the user and the impact of the user community in driving specifications.[28] Thus, this chapter would make an excellent case study for a course in computer usability.

FalconView was the product of an effort by National Guard fighter pilots and Georgia Institute of Technology programmers to support planning for the F-16 Fighting Falcon.[29] The software took advantage of the personal computers that were becoming more widely available during the early 1990s.[30] As with many tools designed by users, FalconView, to use Eric Raymond's words, "scratched an itch," and so it is no surprise that it was quickly and widely adopted.[31] Lindsay details how within a decade of its development, the open-source program had an enthusiastic user base and was deployed in all four services.[32] The numerous examples he provides reveal how the changing nature of the military mission fed development of the FalconView software and the ways in which user input and control were integral to the software's success.

Previously, the military bureaucracy had committed to using a UNIX-based system, MSS, that Tactical Air Command had begun developing in the 1980s for mission planning.[33] At the time, the system ran on very large machines, such that they required "four people to lift [them] and a C-130 to transport [them]."[34] This system had loads of features. As Lindsay describes, it had "something for everyone."[35] During the 1991 Persian Gulf War, crews were impressed with the digital mapping the system provided, but not with the shortage of

[28] Lindsay, *Information Technology and Military Power*, 133.

[29] Lindsay, *Information Technology and Military Power*, 113.

[30] The program was a mapping interface for a set of software tools, but the whole set is often referred to as FalconView.

[31] Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (Cambridge, MA: O'Reilly, 1999).

[32] Lindsay, *Information Technology and Military Power*, 113.

[33] Lindsay, *Information Technology and Military Power*, 116.

[34] Lindsay, *Information Technology and Military Power*, 116.

[35] Lindsay, *Information Technology and Military Power*, 116.

machines or the fact that they were frequently down.[36] That is when the FalconView effort started.

Although the military bureaucracy recognized that FalconView was providing value, it saw it functioning as merely a short-term fix until MSS added the appropriate features. Because FalconView, like many user-created systems, had certain weaknesses, including security, many military officials remained firmly committed to a UNIX-based system. Some military officials also viewed FalconView, an upstart project, as a threat to MSS, the official effort. Consequently, they began placing new demands on the program, with the goal of slowing its development.[37]

The bureaucracy failed to see the real innovation FalconView provided. Lindsay's observation that acquisition managers "took the problem [of UNIX machines] to be simply a matter of computer architecture, rather than the bureaucratic nature of the acquisitions process and the dynamic evolution of mission planning requirements" is spot-on.[38] What FalconView actually provided was an innovative, user-based development process. If the military does not understand why systems like MSS fail — and, conversely, why, by 2009, FalconView had 45,000 military users — there will continue to be a mismatch between what personnel want in systems and what the military actually delivers.[39]

Lindsay also includes a discussion of a highly unconstrained context: special operations in Iraq. Early on in the book, Lindsay says he has chosen to prioritize simplicity over providing fully detailed accounts in his case studies. That was a wise choice, but the complexity of the Iraqi case requires Lindsay to provide so much description that it is difficult to keep it all in mind. As a result, I found it somewhat less compelling than the other three cases and in need of some judicious editing that would have included less detail and more narrative. I nevertheless appreciate the depth of first-hand knowledge that Lindsay is able to bring to bear.

[36] Lindsay, *Information Technology and Military Power*, 117.

[37] Lindsay, *Information Technology and Military Power*, 121.

[38] Lindsay, *Information Technology and Military Power*, 127.

[39] Lindsay, *Information Technology and Military Power*, 126.

Lindsay makes a persuasive case for the reasons behind the failure of the Revolution in Military Affairs during the years that followed the initial "victory" in the war. His discussion of the breakdowns in the sociotechnical operating system is compelling. He does an excellent job of describing the complexities involved in integrating the sociotechnical IT system into the military one, given the extremely dynamic situation on the ground.[40] Lindsay demonstrates that the revolution is more or less meaningless unless the "socio" part of the sociotechnical system is really factored in. Along the way, Lindsay shows that organizations tend to optimize what they measure.[41]

Lindsay's final case study, which covers drone use, is excellent, but also wanders a bit. His discussion of the writings of Abdullah bin Mohammed, a senior commander for al-Qaeda in the Arabian Peninsula, on how to deal with American drones is both fascinating and well presented.[42] Likewise, his discussion of how al-Qaeda adapted to the heavy U.S. use of drones is superb.[43] But his lengthy discussion of the legal issues involved in drone targeting and high-level — as in, presidential — oversight are relatively far removed from the dynamic that is the book's main focus.[44] As such, it was distracting.

Conclusion

Lindsay concludes with some valuable recommendations. He makes the obvious, but extremely useful, suggestion that users of technology work with technology designers during development.[45] He also provides serious and thoughtful recommendations about how to support runtime design.[46] His comments about the People's Liberation Army's lack of experience in using IT in wartime situations are important, and the Defense Department should take serious heed of that critically important point.[47] Indeed, although *Information*

[40] Lindsay, *Information Technology and Military Power*, 158–64.
[41] Lindsay, *Information Technology and Military Power*, 155–57.
[42] Lindsay, *Information Technology and Military Power*, 205–07.
[43] Lindsay, *Information Technology and Military Power*, 207.
[44] Lindsay, *Information Technology and Military Power*, 194–203.
[45] Lindsay, *Information Technology and Military Power*, 215.
[46] Lindsay, *Information Technology and Military Power*, 223–24.
[47] Lindsay, *Information Technology and Military Power*, 229.

Technology and Military Power makes clear that the U.S. military still has much to learn about effectively using IT in wartime, the United States has already absorbed a number of important lessons in that area, whereas China lacks the same level of experience.

There is a lot in Lindsay's book: a theory that attempts to explain the set of forces that enable IT to be useful in war; a model for why the value of IT cyclically increases and decreases in war; and four case studies with exceptional levels of detail, all of which make it an excellent study.

At the same time, I do have some concerns about the book. The significant level of detail in some of the case studies and the assumption that the reader will understand certain references about military history raises the question of for whom exactly this book was written. *Information Technology and Military Power* is clearly valuable for those in the security studies, national security, and political science fields, as well as for military personnel. But, because of how it is written, the study reads like a research monograph, rather than as a text that might be useful in, say, an undergraduate or master's level course in national security.

In addition, the book includes a few inaccuracies. To be sure, Eric Raymond did say, "Given enough eyeballs, all bugs are shallow."[48] But open-source software may have quite serious bugs that go undetected for significant periods of time. A serious error in Open SSL — an implementation of SSL/TLS that encrypts https communications — for example, went undiscovered for two years, even though it utilized open-source code. This error, Heartbleed, made it possible to sometimes read supposedly encrypted text.[49] In addition, although former al-Qaeda member Anwar al Awlaki fled the United States, he did not do so because of anti-Muslim sentiment, as Lindsay implies.[50] Instead, he left because the FBI had tracked him visiting prostitutes, and he was concerned that that information would become public.[51] I would also have preferred that Lindsay avoid using the term "deep state" in his

[48] Quoted in Lindsay, *Information Technology and Military Power*, 63.

[49] For information on the Heartbleed Bug, see https://heartbleed.com/.

[50] Lindsay, *Information Technology and Military Power*, 195.

[51] Scott Shane, "The Lessons of Anwar Al-Awlaki," *New York Times Magazine*, Aug. 27, 2015, https://www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html.

discussion of reversion to oversight.[52] Even if the intent was ironic, the use of the term might have the unintended effect of lending truth to a falsehood. Lastly, it is not the Industrial Revolution that has allowed commanders to be miles from the battlefield — it is electronic communications that has permitted this distancing.[53] All of these, however, are quite minor oversights.

In writing *Information Technology and Military Power*, Lindsay did an exceptional job of pulling together work from security studies, political science, cognitive science, and the sociology of technology and science. Ethnographic studies of military behavior are difficult to do, but he did an excellent job in that regard as well. Lindsay, moreover, showcases that he has a terrific understanding of usability issues — indeed, better than some in Silicon Valley. Thus, *Information Technology and Military Power* will be a valuable text for many experts. I very much hope that the military takes heed of it, for it contains some extremely useful lessons.

Susan Landau *is Bridge Professor in Cyber Security and Policy at The Fletcher School and the School of Engineering, Department of Computer Science, at Tufts University and is a visiting professor in the Department of Computer Science at University College London, where she works at the intersection of cyber security, privacy, law, and policy. Landau has testified before Congress and has frequently briefed U.S. and European policymakers on encryption, surveillance, and cyber security issues. She currently serves on the National Academies Forum on Cyber Resilience and the American Academy of Arts and Sciences Committee on International Security Studies. Landau was a 2012 Guggenheim Fellow and is a fellow of the American Association for the Advancement of Science and of the Association for Computing Machinery.*

[52] Lindsay, *Information Technology and Military Power*, 203.

[53] Lindsay, *Information Technology and Military Power*, 208.

3. A Scholar Reflects on War

Derek S. Reveron

War is foggy. Technology promises to lift the fog of war. War is still foggy.

Those familiar with Jon Lindsay's other work may be surprised that *Information Technology and Military Power* is not centrally about cyber warfare, China and cyber security, or coercion in cyberspace.[54] Instead, one of Lindsay's core themes in his latest book is that "[c]ybersecurity can be understood as a second-order program of using information practice to exploit or protect information practice itself."[55] Indeed, this book is primarily about how military organizations develop and use information during war. Lindsay's dependent variable is "information practice," which, in his view, is shaped by the interaction between operational problems and organizational solutions.

Lindsay's main focus is the key question of when technology can lift the fog of war and transform friction into traction in military conflicts. To be successful in an era in which operational centers resemble offices and staff officers face information overload, he believes that military organizations must confront two separate challenges. "The first," he writes, "is the external challenge of understanding and overcoming a willful and reactive opponent in a particular geographical situation. The second is the internal challenge of coordinating all the intellectual and material resources that make it possible to solve the first challenge. To control the enemy, therefore, a military must also control itself."[56]

---

[54] Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020). For a sampling of Lindsay's other writings, see, for example, Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404, https://doi.org/10.1080/09636412.2013.816122; Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015); and Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York: Oxford University Press, 2018), 179–203.

[55] Lindsay, *Information Technology and Military Power*, 12.

[56] Lindsay, *Information Technology and Military Power*, 49.

Lindsay's fundamental goal, then, is to explain both how humans interact with machines and how organizational structure and culture affect performance. In other words, individuals — with their cognitive abilities and limits — rather than technology and machines, are, sensibly, at the forefront of the study. After all, it is commanders and their staffs who generate the innovative solutions to the problems they face and who sustain the cultures that enable people in hidebound institutions to generate the "work-arounds" that allow them to do their jobs better, or who create stultifying cultures that fail to achieve desired outcomes. Further, contemporary operations centers are filled with multiple networks that connect them to other centers all over the world, live surveillance feeds from sensors that help provide situational awareness, and a variety of open-source tools that reduce uncertainty — and individuals are responsible for interpreting, synthesizing, and transmitting conclusions via information technology based on the data that these instruments provide. Given how much goes on in a modern command center where, to use Lindsay's words, "inboxes are flooded with email, schedules are packed with meetings, and users struggle with the programs that are supposed to make them more productive," the book's focus on the role of the users of technology makes sense.[57]

The Cases

Lindsay draws on several literatures, as well as his own experience in the military, to reach his conclusions. Indeed, *Information Technology and Military Power* is truly an interdisciplinary work, covering topics in security studies, political economy, cognition, science and technology studies, and organizational theory. To explain when information practice improves or undermines organizational performance in war, Lindsay relies on four case studies that relate to the application of technology at both the tactical and operational levels: the Battle of Britain and the use of radar in 1940, the introduction of aviation mission planning software (FalconView) in the 1990s, counter-terrorism operations by Naval Special Warfare teams in Iraq from 2003 to 2008, and the development of new airframes for strike and surveillance missions — or "drone campaigns" — after 2001. Although the justifications for Lindsay's case selections are not immediately obvious, the appendix

[57] Lindsay, *Information Technology and Military Power*, 215.

contains an explanation of his methodology that would be valuable to read prior to engaging the cases.

The case on the Battle of Britain is the most useful in the study for thinking about interstate war. It is, moreover, the case that is most consistent with the book's theory. Lindsay convincingly juxtaposes the Royal Air Force Fighter Command's information practices with those of the German *Luftwaffe* to describe why the United Kingdom ultimately gained the upper hand.

Lindsay's other cases are largely U.S.-centric and, unfortunately, lack the equivalent of the German analogue from his examination of the Battle of Britain, which makes it difficult to compare the information practices of the American military and its main adversaries. Undoubtedly, accessing the information practices of Iraqi insurgents or international terrorists would be nearly impossible. But since one of Lindsay's main goals is to understand the role of information in victory, war must be framed as an interactive competition to understand fully why the U.S. military has struggled against adversaries that lack information-age capabilities.[58] As Lindsay observes, "War is a contest of control in which combatants compete in the construction and destruction of the systems that enable them to know and influence each other … . Each combatant is part of the environment for the other … . Each tries to improve and protect the data systems on which they rely."[59]

Nevertheless, the case studies are rich enough to discern why some organizations succeed at managing information well, while others fail. Lindsay was able to rely on his personal experiences from Kosovo and Iraq, as well as interviews, to bring some needed texture to understanding warfare at an organizational level. The obvious pitfall of being a practitioner-observer is to assume one's experience is generalizable, ignoring Rufus Miles' adage that "[w]here you stand depends on where you sit."[60] But Lindsay is able to remain true to his focus on explaining why information practice and organizational culture support or

[58] On strategic interaction and the causes of war, see James Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995): 379–414, https://www.jstor.org/stable/2706903.

[59] Lindsay, *Information Technology and Military Power*, 50.

[60] Rufus E. Miles, Jr., "The Origin and Meaning of Miles' Law," *Public Administration Review* 38, no. 5 (September/October 1978): 399, https://doi.org/10.2307/975497.

undermine broader objectives. This had to be all the more challenging given how fragmented targeting was during Operation Allied Force and the ways in which special operations doctrine continued to evolve after Lindsay served in Iraq from 2007 to 2008.[61]

In his discussion of Iraq, Lindsay classifies the Special Operations Task Force as an organization pursuing "insulated practice,"[62] which he defines as the product of an institutionalized solution and an unconstrained problem.[63] U.S. conventional forces, coalition partners, and diplomacy and development experts, however, conducted significantly different missions from that of the task force. To test his theory more convincingly, a chapter on conventional forces — beyond Lindsay's relatively short treatment of the Marine Expeditionary Force — in the same battle space during the same time period examining how different organizations fared under the same conditions and within a common strategic context would have been useful. Did the Special Operations Task Force really fail due to its "direct action" focus and information practice, or was it just doing its part to complement other organizations in the same battlespace?[64] Likewise, how did Army-led operations elsewhere compare? If Lindsay is right in his belief that the task force's ingrained preference for direct action was a poor fit for the irregular situation in Anbar, where "indirect action had been and would continue to be critical for the stabilization of the province," why is this not a failure of military strategy, rather than "problematic practice reinforcing insulation"?[65]

---

[61] I worked for the commander of Operation Allied Force as a briefer at the Supreme Headquarters Allied Powers Europe, and the concern I noted with respect to targeting was ensuring that the political coalition remained intact. See Derek S. Reveron, "Coalition Warfare: The Commander's Role," *Defense and Security Analysis* 18, no. 2 (2002): 107–21, https://doi.org/10.1080/14751790220132538. A group of officers who served in the operation later recounted how their views varied depending on the level at which they served. See Stephen D. Wrage, *Immaculate Warfare: Participants Reflect on the Air Campaigns over Kosovo, Afghanistan, and Iraq* (Westport, CT: Praeger, 2003).

[62] Lindsay, *Information Technology and Military Practice*, 136.

[63] Lindsay, *Information Technology and Military Practice*, 10.

[64] Lindsay, *Information Technology and Military Practice*, 142.

[65] Lindsay, *Information Technology and Military Practice*, 153–54.

Implications and Key Questions

At one point, Lindsay critiques analysts' efforts to map insurgent networks that resembled giant "hairballs."[66] However, one could make a similar point about efforts to understand where one's own organization is in the organizational and coalition hierarchy. The relatively straightforward organizational chart that Lindsay provides showing where the Special Operations Task Force fits into the overall system belies the complexity of decision-making and understates internal challenges, which, as he rightly points out, can limit an organization's ability to help execute the larger strategy.[67] This may be the fundamental challenge to his conclusion that "adaptive practice works best when it tackles localized problems that can be solved without interfering with other locales."[68]

This, in turn, raises the question: How scalable are Lindsay's solutions for a national security system as large as the one run by the U.S. government with over three million people and for challenges as complex as wars that regularly include multiple countries? I was part of a team that created a formal institution for the Navy Reserves at the Office of Naval Intelligence to codify Lindsay's and others' early experiences of deploying with Naval Special Warfare. This was an effort to move beyond the pick-up teams that Lindsay mentions and to develop the skills that he identifies in his critique. Even before the publication of this book, I knew Lindsay's views from his field reports. We took his recommendations seriously, recruiting hacker-geniuses from across the country (we called them "tactically proficient" and "analytically superior") and developing a program that provided training for personnel to be integrated more easily into the Special Operations Task Force and the larger intelligence enterprise. This was an important shift that took many years — the program's goals were never fully achieved — and which could be explored further to understand the interactions between the internal and external environments that promote organizational learning. We also found that the combat zone changed so rapidly that it was difficult to keep up with the different skill sets that were needed.

[66] Lindsay, *Information Technology and Military Practice*, 162.

[67] For a copy of the chart, see Lindsay, *Information Technology and Military Practice*, 146.

[68] Lindsay, *Information Technology and Military Practice*, 226.

Lindsay's thesis, then, raises important questions related to the idea of organizational learning, especially the key issue of how military organizations apply the lessons that they learn.[69] Are military organizations, to use Lindsay's phrasing, destined to cycle "through all four patterns in a canonical sequence — managed, insulated, adaptive, and problematic"?[70] It would be important to know where a given organization is in the cycle and how the internal and external environments impact information practice, so that unsynchronized files can get updated rather than archived. In Lindsay's view, leaders and systems integrators must "accept the inevitability of friction and compromise" and rely on a system that supports hacker-geniuses, but he acknowledges that it is a "complicated balancing act in practice."[71]

To build upon Lindsay's work, it would be useful to examine how strategy meets organizational culture and behavior. Admittedly, this book focuses on the tactical and operational levels of war, and on how organizations deal with information. But knowing Lindsay's other work, it would be good to draw out implications at the strategic level. For example, chapter five of the book can be read as a critique of Naval Special Warfare. Lindsay would likely answer a resounding "yes" to Defense Secretary Donald Rumsfeld's question, posed early in the Iraq War, "Are we creating more terrorists than we're killing?"[72] That question should have led policymakers to think carefully about the overall utility of capture and kill missions. Lindsay, however, notes that the SEALs successfully lobbied to conduct direct-action missions, whereas the Marines, who also have a strong combat ethos, "promoted bottom-up innovation that enhance[d] control of the province [of Anbar]."[73] How and why, then, did the Marine Expeditionary Force overcome its organizational preference for combat, while Naval Special Warfare did not? When does organizational culture get in the way of implementing a successful strategy?

---

[69] On this issue, see, for example, Trent Hone, *Learning War: The Evolution of Fighting Doctrine in the U.S. Navy, 1898-1945* (Annapolis, MD: Naval Institute Press, 2018); and Frank G. Hoffman, *Mars Adapting: Military Change During War* (Annapolis, MD: Naval Institute Press, 2021).

[70] Lindsay, *Information Technology and Military Power*, 213.

[71] Lindsay, *Information Technology and Military Power*, 217, 220.

[72] Quoted in Albert R. Hunt, "Killing Terrorists, Creating More," *New York Times,* April 16, 2013, https://www.nytimes.com/2013/04/15/us/letter-killing-terrorists-creating-more.html.

[73] Lindsay, *Information Technology and Military Power*, 178.

Lindsay's examination of information practice in war is revealing, but what are its implications for organizational design in peacetime or during operations short of war? In the book's final chapter, Lindsay provides conclusions about the four categories of information practice that he identifies: performance-enhancing managed practice, performance-improving adaptive practice, performance-undermining problematic practice, and sub-optimizing insulated practice.[74] But can these models be tested in war games and exercises that are realistic enough to help prevent a painful learning process once war starts?

Finally, Lindsay's emphasis on technology's limits to lift the fog of war calls for an explanation of how the obsession with technology originates. It raises the question of whether technology might actually undermine strategic objectives, given the myopic tendency of organizations to focus on carrying out day-to-day operations, rather than on achieving strategic outcomes. In the U.S. context, there is clearly a cultural predilection for technology — the annual defense budget for research, development, testing, and experimentation now exceeds $100 billion annually.[75] Further, industry, Congress, and the military show a preference for new material and technological solutions to perceived operational challenges.

But one of the core contributions of Lindsay's work is that it highlights the importance of non-material solutions to organizational problems and underscores how technology that promises to give the military an advantage can generate uncertainty. Given the United States' poor track record when it comes to achieving strategic results, his conclusions, which challenge the techno-obsessed approach to force development and provide important lessons about service culture and leadership, should be brought to the attention of national security practitioners. After all, the Taliban lacked modern command posts and air power, but it proved capable of re-establishing its sovereignty over Afghanistan despite a 20-year international effort to degrade it and to build up the Afghan state.

---

[74] Lindsay, *Information Technology and Military Power*, 212–42.

[75] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "Defense Budget Overview," May 2021, Table A-1, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf.

While Lindsay's book looks at organizations inside individual countries' militaries, it would also be interesting to consider how the information practices of other militaries perform when operating within the same environment. This could reveal important insights, especially since Lindsay's cases are largely examples of coalition warfare. The Iraq case would be particularly conducive to a comparative approach, given that U.S. special operations forces fought in parallel with troops from the United Kingdom, Australia, New Zealand, and other countries. Perhaps a future project could bring together intelligence officers from several countries to test Lindsay's hypotheses. Similarly, with respect to the drone warfare case, there are many opportunities to look more broadly at the employment of air power: Russia in Syria, Saudi Arabia in Yemen, Israel in Lebanon or Gaza, and coalition strikes in Libya, to name a few. This is, again, a case where bringing officers from different countries together to peer into each other's information practices, where secrecy dominates, could be very helpful analytically.

Conclusion

The goal of *Information Technology and Military Power*, Lindsay writes at the book's outset, is to explain "why organizational and strategic context is the key to understanding the performance of information systems."[76] By this measure, he succeeds and makes an important contribution to the security studies literature by examining how organizations perform relative to the external environment they are trying to shape. For those among the millions of new combat veterans created during the last 20 years who choose to go on to graduate school to try to make sense of their experiences, this book will both serve as a model and help provide a rich understanding of war, the organizations involved in war, where organizations fit into larger enterprises, and the people who fight the wars.

Derek S. Reveron *is professor and chair of the National Security Affairs Department at the U.S. Naval War College and faculty affiliate at the Belfer Center for Science and International Affairs at the Harvard Kennedy School. The views expressed in this*

[76] Lindsay, *Information Technology and Military Power*, 1.

publication are those of the author and do not necessarily reflect the official policy or position of the Naval War College, Department of the Navy, Department of Defense, or the U.S. government.

4. Information Practice: Elegant Theory, Complex Lessons for Military Effectiveness

Jacquelyn Schneider

Jon Lindsay's book, *Information Technology and Military Power*, starts in the 1990s in the "Rumpus Room," a repurposed storage closet housing an intelligence division that used a suite of Microsoft tools to identify Serbian targets.[77] These were the post-Cold War golden years. The United States was a hegemon, fresh off a resounding success in the first Gulf War and buoyed by a booming information technology economy. The U.S. military was a dominant technological force, debuting shock and awe campaigns with long-range and precise GPS-guided munitions, radar-evading stealth aircraft, and networked targeting capabilities. The United States of the Rumpus Room was in the heyday of an emerging "information revolution," ostensibly building information-enabled acquisition strategies and network-centric campaigns to exert information dominance across the globe.

But Lindsay's opening vignette — a tale of bottom-up experimentation with commercial, off-the-shelf information tools — is not a success story. Despite all the information advantages the United States brought to the Kosovo campaign, perhaps the most lasting strategic impact of the effort was a catastrophic information mistake. The accidental U.S. bombing of the Chinese embassy in Belgrade, and the questions it raised over American

[77] Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020).

intent, would plague the U.S.-Chinese relationship for decades. How could a technological behemoth like the United States make such a tremendous mistake?

Lindsay's book sets out to deal with the issue of information technology and military effectiveness by introducing and then examining a concept that he calls "information practice," or the "organizational effort to coordinate knowledge and control."[78] In looking at the variation in successes and failures of information practice, Lindsay presents a deceptively simple two-by-two theory, juxtaposing "constrained" and "unconstrained" external problems with "institutionalized" and "organic" internal solutions. While the theory is certainly elegant, it is Lindsay's ability to trace the complex interdependence of these variables that is the real contribution of the book. Lindsay's capacity to deal with enormous complexity presents the best of a practitioner turned scholar. Indeed, the book represents a clever weaving of theory, history, and studies in contemporary warfare to fill an important vacuum in the literature about information, technology, organizational processes, and, ultimately, military effectiveness. I will highlight below some of the lessons that Lindsay is able to draw out of this complexity and the implications these findings have for our understandings of military innovation, effectiveness, and combat power in the information age.

Key Lessons

First, and perhaps at the highest level of abstraction, Lindsay's case studies demonstrate that information practice can rarely succeed with only a top-down push. This is an important addition to the literature because previous work has often told the story of the great civilian maverick who must catalyze military innovation in the face of cultural stagnation within the armed services.[79] Cavalry officers, charging into machine guns, must

[78] Lindsay, *Information Technology and Military Power*, 2.

[79] For example, see Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984); Edmund Beard, *Developing the ICBM: A Study in Bureaucratic Politics* (New York: Columbia University Press, 1976); Deborah D. Avant, *Political Institutions and Military Change: Lessons from Peripheral Wars* (Ithaca, NY: Cornell University Press, 1994); and Kimberly M. Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955–1991* (Princeton, NJ: Princeton University Press, 1993).

receive a top-down push to abandon their steeds, whereas entrenched service chiefs need a political nudge to abandon the practices that define their service identity.[80]

Interestingly, as Lindsay's review of the technological theory of victory reveals, the information revolution has featured these civilian mavericks in droves — from former Deputy Secretary of Defense Bob Work and the "third offset," to David Deptula and "effects-based operations."[81] Indeed, the era has been defined by a coterie of insiders from Andy Marshall's Office of Net Assessment, who have discovered and branded revolutions in military affairs, and by intellectuals in the Navy who have espoused a technology-based, network-centric warfare.[82] Since Dick Cheney's tenure during the first Bush administration, secretaries of defense have repeatedly extolled the technological revolution of the information age, and the services have, at different points in the last 30 years, pushed new information strategies and information-dependent acquisition programs.[83]

---

[80] Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force* (New Brunswick, NJ: Transaction, 2002); and Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989).

[81] Speech Delivered by Deputy Secretary of Defense Bob Work, "Reagan Defense Forum: The Third Offset Strategy," Nov. 7, 2015, Ronald Reagan Presidential Library, Simi Valley, CA, https://www.defense.gov/Newsroom/Speeches/Speech/Article/628246/reagan-defense-forum-the-third-offset-strategy/; and David A. Deptula, "Effects-Based Operations: Change in the Nature of Warfare," Mitchell Institute for Aerospace Studies, June 1, 2001, https://mitchellaerospacepower.org/effects-based-operations-change-in-the-nature-of-warfare/.

[82] See, for example, Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March/April 1996): 37–54, https://www.foreignaffairs.com/articles/united-states/1996-03-01/revolution-warfare; Andrew F. Krepinevich, Jr., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2002), https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf; Emily Goldman and Thomas Mahnken, eds., *The Information Revolution in Military Affairs in Asia* (New York: Palgrave Macmillan, 2004); and James R. Blaker, *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare* (Westport, CT: Praeger, 2007).

[83] Dick Cheney, *Conduct of the Persian Gulf Conflict: An Interim Report to Congress* (Washington, D.C.: Government Printing Office, 1991); Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* 81, no. 3 (May/June 2002): 20, https://www.foreignaffairs.com/articles/2002-05-01/transforming-military; Ashton Carter, "Department of Defense Accomplishments (2009-2016): Taking the Long View, Investing for the Future," Department of Defense, Jan. 5, 2017, https://dod.defense.gov/Portals/1/Documents/pubs/FINAL-DOD-Exit-Memo.pdf; and Christopher G. Pernin et al., *Lessons from the Army's Future Combat Systems Program* (Santa Monica, CA: RAND Corporation, 2012).

And yet, despite three decades of praise from civilian mavericks, information practice in the U.S. military is mottled. As Christian Brose, a former congressional staffer on the Armed Services Committee, explains,

> Instead of thinking systematically about buying faster, more effective kill chains that could be built now, Washington poured money into newer versions of old military platforms and prayed for technological miracles to come (which often became acquisition debacles when those miracles did not materialize). The result is that U.S. battle networks are not nearly as fast or effective as they have appeared while the United States has been fighting lesser opponents for almost three decades.[84]

Top-down pushes for changes in information practice may have had limited success, but bottom-up experimentation on its own is also not enough. Lindsay's case study of the FalconView program, an example of leveraging user-led information practice to solve a tactical problem, details a mission-planning software that was ultimately replaced because "the traditional acquisition and network management regimes viewed military user development activity as inherently unsustainable and illegitimate."[85] Absent institutional support for the information technology — whether in the form of program management offices or budget requests — innovative programs like FalconView have no potential to scale across the force. Bottom-up information practices may be where true innovation can occur in "unconstrained" situations, but they cannot function effectively in "constrained" environments without some sort of mechanism to link experimentation with top-down support. Indeed, the need to link innovation and institutionalization is not new to information practice. Nina Kollars, for example, has identified a similar dynamic in the development of the gun truck in Vietnam. Without an ability to link the troops on the ground, who were actively developing a solution to a combat tactical problem, to an institutionalized source, successful adaptation could not expand beyond small pockets of innovation.[86]

---

[84] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette, 2020), 3.

[85] Lindsay, *Information Technology and Military Power*, 134.

[86] Nina Kollars, "Military Innovation's Dialectic: Gun Trucks and Rapid Acquisition," *Security Studies* 23, no. 4 (2014): 787–813, https://doi.org/10.1080/09636412.2014.965000.

Both of these related lessons — that top-down pushes for information innovation will fail without bottom-up innovation and that bottom-up innovation cannot scale without institutionalized support — are particularly timely for debates about information practice in contemporary U.S. defense policy. Despite the dominance of tech-friendly secretaries of defense, American investment in information practice has struggled to transition from exquisite technologies in research and development to practical ones for warfighter use and adoption. High-end systems, like the F-35, have promised to overcome the friction of information warfare by integrating automation and enabling "flying clouds" of data transmission. And yet, the jet block upgrade program struggles to keep up with cyber security vulnerabilities — much less optimize information practice with adapted avionics or datalinks. On the bottom-up side of U.S. information practice, there has been an explosion of innovation and information organizations within the Defense Department. Many of these organizations, like the Air Force's Kessel Run or the Defense Department's Defense Digital Service, are tasked with providing exactly the kind of user-based information practice that Lindsay details in his FalconView case. But can these institutions bridge the gap between tactical and strategic operations to create information solutions across organizations and budget cycles?

Related to these top-down and bottom-up lessons about information practice is the profound and intervening role that organizational identities play in the eventual success or failure of information technologies. In particular, Lindsay's chapter comparing counter-insurgency operations and the Army's culture with counter-terrorism missions and the special operations culture reveals the important role that the masks of identity play by filtering information practice.[87] While Carl Builder's work on service identity and military innovation, *The Masks of War*, was written at the outset of the information revolution, its premises remain salient for information practice today.[88] The Air Force, which loves technology and airpower, tends to "weaponize" information practice, turning information operations into sorties and cyber operators into flights that seek the same kinds of strategic effects that dominated the imagination of the Air Force's founding fathers. In contrast, information for the Army is part and parcel of the core ground units, enabling terrestrial campaigns. Meanwhile, for the Navy, information exists primarily as a suite of skills to

[87] Lindsay, *Information Technology and Military Power*, 136–79.

[88] Builder, *The Masks of War*.

support the carrier — competing with, but never as influential as, the operational community identities that shape the Navy's identity.

These organizational identities provide useful organizing impetuses for information practice. They help allocate manpower, determine budgets, and prioritize acquisition strategies. However, without self-awareness, these organizational politics can derail the adoption of information practice. How does the Air Force's weaponization of information help with cyber operations or disinformation campaigns? How can the Navy integrate offensive information into its maritime strategies? Lindsay demonstrates how the quest for information for counter-terrorism operations, a key element of the special operations identity, created tactical successes but did not necessarily help achieve strategic objectives, mostly because the special operations identity struggled to shape information practice in ways that would help accomplish those goals. Organizational lenses can hone information to give a tactical edge, but they can also create blind spots that impede information practice.

Information Technology and Military Power deals mainly with the period that preceded the 2010s. But the era that has followed the tenures of Secretary of Defense Ashton Carter and his deputy, Bob Work, has witnessed the proliferation of new information commands and units, all proffering new approaches to information. While these units were ostensibly created to institutionalize information practice, and thereby provide support and oversight to information efforts, they will inherently create their own bureaucracies and identities as they vie for bigger budgets, manpower, and authorities. How will these new identities interact with the larger organizational politics which are already institutionalized through the armed services and the traditional budget cycle? Can these new organizations transcend their own identities to move from innovation for innovation's sake to true information practice?

Finally, the line between military innovation and military effectiveness is always quite blurry and, in this case, Lindsay's work has implications not only for understanding innovation, but also for military effectiveness in an information age. One of the core assumptions of technology-based theories of military revolutions (especially in the information age) is that technology can overcome information friction. But Lindsay's cases show how difficult (and perhaps impossible) it is to completely reduce information friction.

Even with the introduction of new technologies, the complexities of human interactions in war mean that information is distorted, manipulated, and denied. Early advocates of the information revolution largely overlooked the counter-technologies that would threaten their theories of victory. Instead, they doubled down on information dominance and advocated campaigns of speed, in which flawless technologies would strike decisively, with precision and from increasingly long ranges. These theories sacrificed mass for information on the assumption that better and more information could make up for quantitative asymmetries.

But Lindsay's examination of the Battle of Britain and of information practice in World War II challenges the assumptions of speed and scarcity that underlie technological theories of victory. As Lindsay explains, "C2 improved the efficiency and effectiveness of Fighter Command, but British victory was hardly a simple substitution of information for mass. Many raids got through, and the battle still required a mass of fighters to oppose the Germans."[89] Lindsay's case studies show that information on its own is never enough to ensure military effectiveness. Instead it is the organizations that are able to respond and adapt to information that are most likely to succeed. While not a core premise of the book, Lindsay's theory leaves its readers seeking resilience, rather than dominance, in the face of the information revolution. This resilience may be augmented by new network architectures and technologies, but it can really only be found through human choices about organizational management and user-led innovation.

Conclusion

Information Technology and Military Power's greatest lesson for practitioners and scholars is that information does not exist on its own. Instead, "it is not just the quality of technology that matters in war, but the way in which practitioners use it. The quality of information practice, in turn, depends on the relationship between operational problems and organizational solutions."[90] In the end, this is a book about humans and how humans interact with information (mediated by technology) to create military effectiveness. The

[89] Lindsay, *Information Technology and Military Power*, 107.

[90] Lindsay, *Information Technology and Military Power*, 212.

solutions it proffers are not about doubling down on acquisitions reform or technological capacity. Instead, they are about the self-awareness that militaries require to combat their own human and organizational biases to best utilize technology to create military power.

Jacquelyn Schneider *is a Hoover Fellow at Stanford University, an affiliate at Stanford's Center for International Security and Arms Control, and a non-resident fellow at the Naval War College's Cyber and Innovation Policy Institute. Her research focuses on the intersection of technology, national security, and political psychology, with a special interest in cyber security, unmanned technologies, and military innovation. She was previously a senior policy adviser to the Cyberspace Solarium Commission and currently serves as a reservist in the U.S. Air Force. She has a B.A. from Columbia University, M.A. from Arizona State University, and Ph.D. from George Washington University.*